

Kaspersky Anti-Virus 2010

MANUALE DELL'UTENTE

VERSIONE PROGRAMMA: 9.0 CRITICAL FIX 2



KASPERSKY lab

Gentile utente,

grazie per aver scelto il nostro prodotto. Ci auguriamo che questa documentazione sia utile e fornisca risposte esaustive a gran parte delle domande relative al prodotto software cui è allegata.

Qualsiasi tipo di riproduzione o distribuzione di qualsiasi materiale, incluse le traduzioni, è consentito solo previa autorizzazione scritta concessa da Kaspersky Lab.

Il presente documento e le immagini grafiche correlate possono essere utilizzati a scopo esclusivamente informativo, non commerciale né personale.

Il presente documento è soggetto a modifiche senza ulteriori notifiche. La versione più recente del documento è disponibile nel sito Web di Kaspersky Lab all'indirizzo <http://www.kaspersky.it/docs>.

Kaspersky Lab non si assume responsabilità per il contenuto, la qualità, la pertinenza o la precisione del materiale utilizzato in questo documento i cui diritti appartengono a terze parti o per eventuali danni potenziali associati all'uso di essi.

Il presente documento include marchi registrati e marchi di servizi che sono di proprietà dei rispettivi proprietari.

Data di revisione: 10/8/09

© 1997-2009 Kaspersky Lab ZAO. Tutti i diritti riservati.

<http://www.kaspersky.it>
<http://support.kaspersky.it>

SOMMARIO

INTRODUZIONE	9
Kit di distribuzione	9
Servizi offerti agli utenti registrati	10
Requisiti di sistema hardware e software	10
KASPERSKY ANTI-VIRUS 2010	11
Come ottenere informazioni sull'applicazione	11
Fonti di informazioni per l'esecuzione di ricerche	11
Come contattare l'ufficio vendite	12
Come contattare il servizio di Assistenza tecnica	12
Discussioni sulle applicazioni Kaspersky Lab nel forum Web	13
NOVITÀ DI KASPERSKY ANTI-VIRUS 2010	14
COSA SI INTENDE PER PROTEZIONE DEL COMPUTER	15
Componenti di protezione	15
Attività di scansione anti-virus	17
Aggiornamento	17
Protezione di dati e attività online	17
Procedure guidate e strumenti	18
Funzionalità di assistenza del programma	18
INSTALLAZIONE DI KASPERSKY ANTI-VIRUS	20
Passaggio 1. Ricerca di una versione più recente dell'applicazione	21
Passaggio 2. Verifica dei requisiti di sistema per l'installazione	21
Passaggio 3. Selezione del tipo di installazione	22
Passaggio 4. Visualizzazione del Contratto di licenza	22
Passaggio 5. Informativa sulla Raccolta dati per Kaspersky Security Network	22
Passaggio 6. Selezione della cartella di destinazione	23
Passaggio 7. Selezione dei componenti dell'applicazione per l'installazione	23
Passaggio 8. Utilizzo delle impostazioni dell'applicazione salvate dopo l'installazione precedente	24
Passaggio 9. Ricerca di altre applicazioni anti-virus	24
Passaggio 10. Preparazione finale per l'installazione	25
Passaggio 11. Completamento dell'installazione	25
OPERAZIONI PRELIMINARI	26
Configurazione guidata dell'applicazione	27
Passaggio 1. Attivazione dell'applicazione	27
Passaggio 2. Selezione della modalità di protezione	29
Passaggio 3. Configurazione dell'aggiornamento dell'applicazione	29
Passaggio 4. Limitazione dell'accesso all'applicazione	30
Passaggio 5. Selezione delle minacce da rilevare	30
Passaggio 6. Chiusura della procedura guidata	30
Aggiornamento dell'applicazione	30
Scansione anti-virus del computer	31
Ricerca delle vulnerabilità del computer	31
Gestione della licenza	32
Sottoscrizione per il rinnovo automatico della licenza	32
Partecipazione a Kaspersky Security Network	33

Gestione della protezione	34
Stato della protezione	36
Sospensione della protezione	36
INTERFACCIA DELL'APPLICAZIONE	38
Icona dell'area di notifica	38
Menu di scelta rapida	39
Finestra principale di Kaspersky Anti-Virus	40
Notifiche	42
Finestra delle impostazioni dell'applicazione	42
PROTEZIONE DEL FILE SYSTEM DEL COMPUTER	43
Algoritmo di funzionamento del componente	44
Modifica del livello di protezione per i file e la memoria	45
Modifica delle azioni da eseguire sugli oggetti rilevati	45
Creazione di un ambito di protezione	46
Utilizzo dell'analisi euristica	47
Ottimizzazione della scansione	48
Scansione di file compositi	48
Scansione di file compositi di grandi dimensioni	49
Modifica della modalità di scansione	49
Tecnologia di scansione	50
Sospensione dell'attività del componente: creazione di una pianificazione	50
Sospensione dell'attività del componente: creazione di un elenco di applicazioni	51
Ripristino delle impostazioni di protezione predefinite	52
PROTEZIONE DELLA POSTA	53
Algoritmo di funzionamento del componente	54
Modifica del livello di protezione dei messaggi di posta elettronica	55
Modifica delle azioni da eseguire sugli oggetti rilevati	55
Creazione di un ambito di protezione	56
Scansione della posta elettronica in Microsoft Office Outlook	57
Scansione della posta elettronica in The Bat!	57
Utilizzo dell'analisi euristica	58
Scansione di file compositi	58
Filtraggio degli allegati	59
Ripristino delle impostazioni di protezione predefinite della posta elettronica	59
PROTEZIONE DEL TRAFFICO WEB	60
Algoritmo di funzionamento del componente	61
Modifica del livello di protezione del traffico HTTP	62
Modifica delle azioni da eseguire sugli oggetti rilevati	62
Creazione di un ambito di protezione	63
Selezione del tipo di scansione	63
Barra degli strumenti degli URL di Kaspersky	64
Utilizzo dell'analisi euristica	65
Ottimizzazione della scansione	66
Ripristino delle impostazioni di protezione Web predefinite	66
PROTEZIONE DEL TRAFFICO DEI PROGRAMMI DI MESSAGGISTICA ISTANTANEA	67
Algoritmo di funzionamento del componente	68
Creazione di un ambito di protezione	68

Selezione del metodo di scansione	68
Utilizzo dell'analisi euristica	69
DIFESA PROATTIVA	70
Utilizzo dell'elenco di attività pericolose	70
Modifica delle regole per il monitoraggio delle attività pericolose	71
Creazione di un gruppo di applicazioni attendibili	72
Controllo degli account di sistema	72
SCANSIONE DEL COMPUTER	73
Scansione anti-virus	73
Avvio dell'attività di scansione anti-virus	75
Creazione di un collegamento per l'esecuzione di attività	76
Creazione di un elenco di oggetti da esaminare	76
Modifica del livello di protezione.....	77
Modifica delle azioni da eseguire sugli oggetti rilevati	77
Modifica del tipo di oggetti da esaminare	78
Ottimizzazione della scansione	79
Scansione di unità disco rimovibili.....	79
Scansione di file compositi	80
Tecnologia di scansione.....	81
Modifica del metodo di scansione	81
Modalità di esecuzione: creazione di una pianificazione	82
Modalità di esecuzione: specifica di un account.....	83
Funzionalità dell'avvio pianificato delle attività	83
Ripristino delle impostazioni di scansione predefinite	83
Scansione Vulnerabilità	84
Avvio dell'attività di ricerca delle vulnerabilità.....	85
Creazione di un collegamento per l'esecuzione di attività	85
Creazione di un elenco di oggetti da esaminare	85
Modalità di esecuzione: creazione di una pianificazione	86
Modalità di esecuzione: specifica di un account.....	87
AGGIORNAMENTO	88
Avvio dell'aggiornamento.....	89
Rollback dell'ultimo aggiornamento	90
Selezione di una sorgente degli aggiornamenti	90
Utilizzo di un server proxy	91
Impostazioni internazionali.....	91
Azioni da eseguire dopo l'aggiornamento	91
Aggiornamento da una cartella locale.....	92
Modifica della modalità di esecuzione dell'attività di aggiornamento	93
Esecuzione degli aggiornamenti utilizzando un altro account utente.....	93
CONFIGURAZIONE IMPOSTAZIONI APPLICAZIONE	94
Protezione.....	95
Abilitazione/disabilitazione della protezione del computer	96
Avvio di Kaspersky Anti-Virus all'avvio del sistema operativo	96
Utilizzo della modalità di protezione interattiva.....	97
Limitazione dell'accesso a Kaspersky Anti-Virus.....	97
Anti-Virus File	98

Anti-Virus Posta	99
Anti-Virus Web	99
Anti-Virus IM	100
Difesa Proattiva	101
Scansione	101
Aggiornamento	102
Impostazioni	103
Auto-difesa di Kaspersky Anti-Virus	103
Tecnologia avanzata di disinfezione	104
Utilizzo di Kaspersky Anti-Virus su un computer portatile	104
Prestazioni del computer durante l'esecuzione delle attività	104
Esportazione/importazione delle impostazioni di Kaspersky Anti-Virus	105
Ripristino delle impostazioni predefinite	105
Minacce ed esclusioni	106
Rete	110
Notifiche	114
Rapporti e Backup	115
Feedback	119
Aspetto dell'applicazione	119
Utilizzo dei profili di Kaspersky Anti-Virus	121
FUNZIONI AVANZATE	122
Tastiera Virtuale	122
Disco di ripristino	123
Creazione del Disco di Ripristino	124
Avvio del computer attraverso il Disco di Ripristino	124
Configurazione del browser	125
Ripristino dopo un'infezione	126
Pulizia guidata dei dati riservati	127
RAPPORTI	128
Selezione di un componente o di un'attività per creare un rapporto	129
Gestione del raggruppamento delle informazioni nel rapporto	129
Notifica sul completamento del rapporto	130
Selezione dei tipi di evento	130
Visualizzazione dei dati sullo schermo	131
Visualizzazione delle informazioni statistiche avanzate	132
Salvataggio di un rapporto in un file	132
Utilizzo del filtraggio complesso	133
Ricerca eventi	134
NOTIFICHE	135
Rilevamento di un oggetto dannoso	136
Impossibile disinfettare l'oggetto	137
Richiesta di esecuzione di una procedura speciale	137
Rilevamento di un oggetto pericoloso nel traffico	137
Rilevamento di un oggetto sospetto	138
Rilevamento di un'attività pericolosa nel sistema	139
Rilevamento di processi nascosti	139
Rilevamento di un tentativo di accesso al Registro di sistema	140
Rilevamento di un attacco di phishing	140

Rilevamento di un collegamento sospetto	141
Rilevamento di un certificato non valido.....	141
CONVALIDA DELLE IMPOSTAZIONI DI KASPERSKY ANTI-VIRUS	142
"Virus" di prova EICAR e sue varianti	142
Test della protezione del traffico HTTP.....	143
Test della protezione del traffico SMTP	144
Convalida delle impostazioni di Anti-Virus File	144
Convalida delle impostazioni dell'attività di scansione anti-virus.....	144
UTILIZZO DELL'APPLICAZIONE DALLA RIGA DI COMANDO.....	145
Gestione dei componenti e delle attività dell'applicazione	146
Scansione anti-virus	148
Aggiornamento dell'applicazione	151
Rollback dell'ultimo aggiornamento	151
Esportazione delle impostazioni di protezione	152
Importazione delle impostazioni di protezione	152
Avvio dell'applicazione	152
Arresto dell'applicazione	153
Creazione di un file di traccia	153
Visualizzazione della Guida	153
Codici restituiti della riga di comando	154
RISOLUZIONE DEI PROBLEMI.....	155
Creazione di un rapporto sullo stato del sistema	156
Creazione di un file di traccia	156
Invio di file di dati	157
Esecuzione di script AVZ	158
INFORMATIVA SULLA RACCOLTA DATI PER KASPERSKY SECURITY NETWORK.....	159
UTILIZZO DI CODICE DI TERZE PARTI	163
Libreria Crypto C (libreria di software per la protezione dei dati)	164
Libreria Fastscript 1.9	164
Libreria libnkfm 7.4.7.7	164
Libreria del parser Bison GNU	165
Libreria AGG 2.4	165
Libreria OpenSSL 0.9.8d	166
Libreria Gecko SDK 1.8	167
Libreria Zlib 1.2	167
Libreria libpng 1.2.8, 1.2.29	167
Libreria Libnkfm 2.0.5	167
Libreria Expat 1.2, 2.0.1	168
Libreria Info-ZIP 5.51	168
Libreria Windows Installer XML (WiX) 2.0.....	169
Libreria Passthru.....	171
Libreria Filter.....	171
Libreria Netcfg	172
Libreria Pcre 3.0	172
Libreria RFC1321-based (RSA-free) MD5.....	172
Libreria Windows Template (WTL 7.5).....	172
Libreria Libjpeg 6b	175

Libreria Libungif 3.0	176
Libreria Libxdr	176
Libreria Tiniconv - 1.0.0	177
Libreria Bzip2/libbzip2 1.0.5	182
Libreria Libspf2-1.2.9	182
Libreria Protocol Buffer	183
GLOSSARIO	184
KASPERSKY LAB	191
CONTRATTO DI LICENZA	192
INDICE	198

INTRODUZIONE

IN QUESTA SEZIONE:

Kit di distribuzione	9
Servizi offerti agli utenti registrati.....	9
Requisiti di sistema hardware e software	10

KIT DI DISTRIBUZIONE

È possibile acquistare la versione in scatola di Kaspersky Anti-Virus presso i nostri partner oppure online dai negozi su Internet, ad esempio nella sezione **Compra Online** del sito <http://www.kaspersky.it>.

Il pacchetto della versione in scatola del programma include:

- Una busta sigillata con il CD di installazione contenente i file del programma e la documentazione in formato PDF.
- La documentazione in formato stampato, ovvero il Manuale dell'utente e la Guida introduttiva.
- Il Contratto di licenza (a seconda del paese).
- La scheda di attivazione contenente un codice di attivazione e il manuale di attivazione dell'applicazione (a seconda del paese).

Il Contratto di licenza con l'utente finale (EULA) è un contratto legale che intercorre tra l'utente e Kaspersky Lab, in cui si specificano le condizioni di utilizzo del software acquistato.

L'EULA deve essere letto con molta attenzione.

Se non si accettano le condizioni dell'EULA, è possibile restituire la confezione del prodotto al partner presso il quale è stata acquistata e ottenere il rimborso corrispondente all'importo pagato, a condizione che la busta contenente il disco di installazione sia ancora sigillata.

L'apertura del disco di installazione sigillato implica l'accettazione delle condizioni dell'EULA.

Si consiglia pertanto di leggere attentamente le condizioni dell'EULA prima di aprire la busta.

L'acquisto di Kaspersky Anti-Virus presso il negozio online comporta il download del prodotto dal sito Web di Kaspersky Lab. Il presente Manuale dell'utente è incluso nel pacchetto di installazione. Alla ricezione del pagamento, l'utente riceverà un messaggio di posta elettronica con il codice di attivazione.

SERVIZI OFFERTI AGLI UTENTI REGISTRATI

Kaspersky Lab offre un pacchetto completo di servizi a tutti gli utenti legalmente registrati consentendo loro di potenziare le prestazioni dell'applicazione.

Con l'acquisto di una licenza si diventa utente registrato e si può usufruire durante tutto il periodo di durata della licenza dei servizi seguenti:

- aggiornamenti orari dei database dell'applicazione e aggiornamento al pacchetto software;
- supporto per i problemi correlati all'installazione, alla configurazione e all'utilizzo del prodotto software acquistato. I servizi vengono forniti tramite telefono o posta elettronica;
- notifiche relative ai nuovi prodotti Kaspersky Lab e ai nuovi virus che si diffondono in tutto il mondo. Questo servizio è disponibile per gli utenti che hanno effettuato la sottoscrizione alla mailing list delle news di Kaspersky Lab nel sito Web del Servizio di assistenza tecnica (<http://support.kaspersky.it/subscribe>).

Non viene fornito supporto per i problemi correlati alle prestazioni e all'utilizzo dei sistemi operativi o di altre tecnologie non Kaspersky.

REQUISITI DI SISTEMA HARDWARE E SOFTWARE

Per il corretto funzionamento di Kaspersky Anti-Virus 2010, il computer deve soddisfare i requisiti minimi seguenti:

Requisiti generali:

- 375 MB di spazio libero su disco rigido.
- unità CD-ROM (per l'installazione di Kaspersky Anti-Virus 2010 dal CD di installazione).
- Microsoft Internet Explorer 6.0 o versione successiva (per l'aggiornamento dei database dell'applicazione e dei moduli software via Internet).
- Microsoft Windows Installer 2.0.
- *Microsoft Windows XP Home Edition (Service Pack 2), Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition:*
 - processore Intel Pentium da 300 MHz o superiore (o un equivalente compatibile).
 - 256 MB di RAM libera.
- *Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:*
 - processore Intel Pentium da 800 MHz 32 bit (x86) / 64-bit (x64) o superiore (o un equivalente compatibile).
 - 512 MB di RAM libera.
- *Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:*
 - processore Intel Pentium da 1 GHz 32 bit (x86) / 64 bit (x64) o superiore (o un equivalente compatibile).
 - 1 GB di RAM libera (32 bit); 2 GB di RAM libera (64 bit).

KASPERSKY ANTI-VIRUS 2010

Kaspersky Anti-Virus 2010 rappresenta una soluzione all'avanguardia per la protezione dei dati.

Ciò che distingue Kaspersky Anti-Virus 2010 da tutti gli altri software, persino dagli altri prodotti Kaspersky Lab, è la completezza della protezione dei dati del computer dell'utente.

IN QUESTA SEZIONE:

Come ottenere informazioni sull'applicazione.....[11](#)

COME OTTENERE INFORMAZIONI SULL'APPLICAZIONE

L'utente ha a disposizione le risposte più appropriate a tutte le domande relative all'acquisto, all'installazione o all'utilizzo dell'applicazione.

Kaspersky Lab offre varie fonti di informazioni relative all'applicazione. L'utente sceglierà quelle più adatte in base al livello di importanza e urgenza delle domande.

IN QUESTA SEZIONE:

Fonti di informazioni per l'esecuzione di ricerche[11](#)

Come contattare l'ufficio vendite.....[12](#)

Come contattare il servizio di Assistenza tecnica[12](#)

Discussioni sulle applicazioni Kaspersky Lab nel forum Web[13](#)

FONTI DI INFORMAZIONI PER L'ESECUZIONE DI RICERCHE

È possibile fare riferimento alle fonti di informazioni relative all'applicazione seguenti:

- pagina dell'applicazione nel sito Web di Kaspersky Lab;
- pagina dell'applicazione nel sito Web del Servizio di assistenza tecnica (nella Knowledge Base);
- pagina di servizio dell'assistenza FastTrack;
- Guida;
- documentazione.

Pagina dell'applicazione nel sito Web di Kaspersky Lab

http://www.kaspersky.com/it/kaspersky_anti-virus

In questa pagina vengono fornite informazioni generali sull'applicazione e sulle relative funzionalità e opzioni.

Pagina dell'applicazione nel sito Web del Servizio di assistenza tecnica (Knowledge Base)

<http://support.kaspersky.it/kav2010>

In questa pagina sono disponibili gli articoli creati dagli specialisti del Servizio di assistenza tecnica.

Tali articoli contengono informazioni utili, suggerimenti e domande frequenti sull'acquisto, l'installazione e l'utilizzo dell'applicazione. Gli articoli sono ordinati in base all'argomento, ad esempio Gestione dei file chiave, Impostazione degli aggiornamenti dei database o Eliminazione degli errori di funzionamento. Possono fornire risposte alle domande che riguardano non solo questa applicazione ma anche gli altri prodotti Kaspersky Lab, nonché includere le novità del Servizio di assistenza tecnica.

Servizio di assistenza FastTrack

In questa pagina di servizio è possibile trovare le domande frequenti poste dagli utenti con le relative risposte, aggiornate regolarmente. Per utilizzare questo servizio, è necessario disporre di una connessione Internet.

Per accedere alla pagina di servizio, nella pagina principale dell'applicazione cliccare sul collegamento **Assistenza** e, nella finestra visualizzata, cliccare sul bottone relativo all'assistenza **Fast Track**.

Guida

Il pacchetto di installazione dell'applicazione include il file della Guida completo e sensibile al contesto contenente le informazioni relative alla gestione della protezione del computer (visualizzazione dello stato di protezione, scansione di varie aree del computer per la rilevazione di virus, esecuzione di altre attività), nonché informazioni su ciascuna finestra dell'applicazione, ad esempio l'elenco delle specifiche impostazioni con relativa descrizione e l'elenco delle attività da eseguire.

Per aprire il file della Guida, cliccare sul bottone **Guida** nella finestra desiderata oppure premere il tasto <F1>.

Documentazione

Il pacchetto di installazione di Kaspersky Anti-Virus include il documento **Manuale dell'utente** (in formato PDF). Tale documento contiene descrizioni delle opzioni e delle funzionalità dell'applicazione, nonché i principali algoritmi di funzionamento.

COME CONTATTARE L'UFFICIO VENDITE

In caso di domande riguardanti la scelta o l'acquisto dell'applicazione o l'estensione della licenza, è possibile rivolgersi all'indirizzo email:

sales.consumer@it.kaspersky.com.

COME CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA

Una volta acquistato Kaspersky Anti-Virus, è possibile ottenere tutte le informazioni desiderate dal servizio di Assistenza tecnica telefonicamente o tramite Internet.

Gli specialisti del servizio di Assistenza tecnica saranno lieti di rispondere a qualsiasi domanda relativa all'installazione e all'utilizzo dell'applicazione. Saranno inoltre pronti a supportarvi nella risoluzione dei problemi derivanti dalle attività del malware nel caso in cui il vostro computer sia stato infettato.

Prima di contattare il servizio di Assistenza tecnica, leggere le regole dell'Assistenza tecnica relative ai prodotti Kaspersky Lab (<http://support.kaspersky.it/support/rules>).

Richiesta via e-mail al servizio di Assistenza tecnica

La domanda può essere formulata in russo, inglese, tedesco, francese o spagnolo.

La risposta del servizio di Assistenza tecnica alla richiesta sarà inviata all'account Kaspersky dell'utente (<https://my.kaspersky.com>) e all'indirizzo di posta elettronica specificato nella richiesta.

Descrivere il più dettagliatamente possibile il problema riscontrato nel modulo di richiesta Web. Compilare i seguenti campi obbligatori:

- **Tipo di richiesta.** Selezionare l'oggetto che più si avvicina al problema, ad esempio: Problema di installazione/disinstallazione del prodotto oppure Problema di ricerca/eliminazione di virus. Se l'argomento desiderato non è disponibile, selezionare "Domanda di carattere generale".
- **Nome e numero di versione dell'applicazione.**
- **Testo della richiesta.** Descrivere il problema rilevato il più dettagliatamente possibile.
- **ID cliente e password.** Specificare il numero cliente e la password ricevuti durante la registrazione nel sito Web del servizio di Assistenza tecnica.
- **Indirizzo e-mail.** Il servizio di Assistenza tecnica invierà una risposta alle domande formulate all'indirizzo specificato.

Assistenza tecnica telefonica

Per sottoporre un problema urgente, è possibile contattare telefonicamente il servizio di Assistenza tecnica (<http://www.kaspersky.com/it/contacts>). Prima di chiamare gli specialisti dell'Assistenza tecnica, raccogliere le informazioni (<http://support.kaspersky.com/support/details>) relative al computer e all'applicazione anti-virus installata. Tali informazioni semplificheranno il compito degli specialisti.

DISCUSSIONI SULLE APPLICAZIONI KASPERSKY LAB NEL FORUM WEB

Se la domanda non richiede una risposta urgente, è possibile sottoporla agli specialisti di Kaspersky Lab e ad altri utenti nei forum Kaspersky all'indirizzo <http://forum.kaspersky.com>.

In questo forum è possibile visualizzare gli argomenti esistenti, lasciare commenti, creare nuovi argomenti e utilizzare il motore di ricerca.

NOVITÀ DI KASPERSKY ANTI-VIRUS 2010

Kaspersky Anti-Virus 2010 è uno strumento completo di protezione dei dati. Questa forma di protezione copre tutti i canali di scambio e trasferimento dati. La configurazione flessibile, disponibile per qualsiasi componente, consente agli utenti di adattare con efficacia Kaspersky Anti-Virus alle proprie specifiche esigenze.

Di seguito vengono descritte in modo dettagliato le nuove funzionalità di Kaspersky Anti-Virus 2010.

Nuovo componente di protezione:

- Il nuovo componente Anti-Virus IM (vedere pagina [67](#)) garantisce la protezione della messaggistica istantanea. Eseguendo la scansione dei messaggi alla ricerca di oggetti dannosi.
- Kaspersky Anti-Virus include la barra degli strumenti degli URL di Kaspersky (vedere pagina [64](#)) gestito da Anti-Virus Web. Tale modulo verifica se i collegamenti presenti nella pagina Web appartengono all'elenco degli indirizzi Web di phishing o sospetti. Questo modulo è incorporato come plug-in nei browser Microsoft Internet Explorer e Mozilla Firefox.
- Il monitoraggio dell'accesso ai siti Web di phishing e la protezione da attacchi di phishing vengono eseguiti mediante la scansione dei collegamenti presenti nei messaggi e nelle pagine Web, nonché mediante l'utilizzo del database degli indirizzi di phishing quando viene rilevato un tentativo di accedere ai siti Web. È possibile verificare che gli indirizzi Web non siano inclusi nell'elenco degli indirizzi Web di phishing. Questa opzione è disponibile solo per Anti-Virus Web (vedere pagina [63](#)), e Anti-Virus IM (vedere pagina [68](#)).
- Un nuovo strumento denominato Scansione Vulnerabilità (vedere pagina [84](#)) è stato aggiunto all'elenco delle attività di scansione. Tale strumento semplifica l'individuazione e l'eliminazione delle vulnerabilità e delle minacce alla protezione nelle applicazioni installate nel computer e nelle impostazioni del sistema operativo.

Nuovo componente dell'interfaccia:

- È stato implementato un nuovo approccio alla gestione della protezione denominato Protezione. La protezione del computer è garantita in tre direzioni diverse: file dell'utente e dati personali, oggetti del sistema operativo e applicazioni installate nel computer, nonché attività di rete. A ognuna delle direzioni di protezione è applicato un insieme specifico di componenti di Kaspersky Anti-Virus. Grazie al componente Protezione, l'utente può individuare il componente che offre protezione per una determinata categoria di risorse e passare rapidamente alla modifica delle rispettive impostazioni.
- Procedure guidate e strumenti (vedere pagina [18](#)), che supportano l'utente nell'esecuzione di attività specifiche mirate a garantire protezione al computer, sono raggruppati nella sezione **Protezione+**.

COSA SI INTENDE PER PROTEZIONE DEL COMPUTER

Kaspersky Anti-Virus garantisce protezione al computer da minacce nuove o note. Ogni tipo di minaccia viene elaborato da un componente distinto dell'applicazione. Ciò rende la configurazione un processo flessibile che offre opzioni di configurazione semplici per tutti i componenti, in modo da soddisfare le esigenze di utenti specifici o di intere aziende.

Kaspersky Anti-Virus include gli strumenti di protezione seguenti:

- Componenti (vedere pagina [15](#)) che offrono protezione per:
 - file e dati personali;
 - sistema;
 - attività di rete.
- Attività di scansione anti-virus (vedere pagina [17](#)), che consentono di esaminare singoli file, cartelle, unità o aree alla ricerca di virus o di eseguire una scansione completa del computer.
- Aggiornamento (vedere pagina [17](#)), che garantisce che i moduli interni e i database dell'applicazione siano aggiornati.
- Procedure guidate e strumenti (vedere pagina [18](#)), che facilitano l'esecuzione delle attività durante il funzionamento di Kaspersky Anti-Virus.
- Funzioni di assistenza (vedere pagina [18](#)) che forniscono supporto informativo per l'utilizzo del programma e l'espansione delle relative funzionalità.

IN QUESTA SEZIONE:

Componenti di protezione.....	15
Attività di scansione anti-virus	17
Aggiornamento	17
Protezione di dati e attività online	17
Procedure guidate e strumenti	18
Funzionalità di assistenza del programma	18

COMPONENTI DI PROTEZIONE

I componenti di protezione seguenti offrono una difesa al computer in tempo reale:

Anti-Virus File (vedere pagina [43](#))

Anti-Virus File monitora il file system del computer. Esegue la scansione di tutti i file che possono essere aperti, eseguiti o salvati nel computer e di tutte le unità disco collegate. Kaspersky Anti-Virus intercetta ogni tentativo di accedere a un file e ne esegue la scansione allo scopo di individuare virus noti. Il file può essere ulteriormente elaborato solo se non è infetto o se non determina errori nell'applicazione. Se per qualsiasi motivo un file non può essere disinfettato, verrà eliminato e ne verrà salvata una copia nel backup oppure verrà spostato in quarantena.

Anti-Virus Posta (vedere pagina [53](#))

Anti-Virus Posta esamina tutti i messaggi di posta elettronica in entrata e in uscita del computer. Analizza i messaggi di posta alla ricerca di programmi dannosi. Il messaggio di posta è disponibile per il destinatario solo se non contiene oggetti pericolosi. Il componente inoltre analizza i messaggi di posta elettronica per rilevare phishing.

Anti-Virus Web (vedere pagina [60](#))

Anti-Virus Web intercetta e blocca gli script nei siti Web se costituiscono una minaccia. Tutto il traffico HTTP è sottoposto a un attento esame. Il componente inoltre analizza le pagine Web per rilevare phishing.

Anti-Virus IM (vedere pagina [67](#))

Anti-Virus IM garantisce un utilizzo sicuro delle pagine Internet. Il componente protegge le informazioni che il computer riceve tramite i protocolli IM e garantisce il funzionamento sicuro della messaggistica istantanea.

Anti-Phishing

Si tratta di un componente, integrato in Anti-Virus Web e Anti-Virus IM, che consente di verificare se gli indirizzi Web sono inclusi nell'elenco di indirizzi Web sospetti e di phishing.

Alcuni componenti di protezione sono disponibili solo in Kaspersky Internet Security 2010, tra cui:

Controllo Applicazioni

Il componente Controllo Applicazioni registra le azioni eseguite dalle applicazioni nel sistema e ne gestisce le attività in base al gruppo al quale vengono assegnate. Per ciascun gruppo di applicazioni viene definito un insieme di regole. Tali regole gestiscono l'accesso delle applicazioni a varie risorse.

Firewall

Il Firewall garantisce la protezione del lavoro nelle reti locali e in Internet. Tale componente filtra tutte le attività di rete utilizzando regole di due tipi: *regole dell'applicazione* e *regole per i pacchetti*.

Difesa Proattiva (vedere pagina [70](#))

Difesa Proattiva consente di rilevare un nuovo programma dannoso prima che esegua la propria attività. Il componente è stato progettato per il monitoraggio e l'analisi del comportamento di tutte le applicazioni installate nel computer. Kaspersky Anti-Virus decide se l'applicazione è potenzialmente pericolosa in base alle azioni che essa esegue. Il computer è pertanto protetto non solo dai virus noti ma anche da quelli nuovi, nonché da quelli che non sono stati ancora scoperti.

Prevenzione Intrusioni

Prevenzione Intrusioni viene caricato all'avvio del sistema operativo e tiene traccia del traffico di rete in entrata alla ricerca di attività tipiche degli attacchi di rete. In seguito all'individuazione di un tentativo di attacco al computer, Kaspersky Anti-Virus blocca tutte le attività di rete del computer da cui proviene l'attacco verso il computer in uso.

Anti-Spam

Anti-Spam è integrato nel client di posta installato nel computer e monitora tutti i messaggi di posta elettronica in entrata per cercare eventuale spam. Tutti i messaggi contenenti spam vengono contrassegnati con un'intestazione speciale. È inoltre possibile configurare Anti-Spam per l'elaborazione dello spam (eliminazione automatica, spostamento in una cartella speciale e così via). Il componente inoltre analizza i messaggi di posta elettronica per rilevare phishing.

Monitor di Rete

Il componente è stato progettato per visualizzare informazioni sulle attività di rete in modalità in tempo reale.

Anti-Banner

Anti-Banner blocca le informazioni pubblicitarie contenute nei banner incorporati nelle interfacce di vari programmi installati nel computer o visualizzate online.

Filtro Genitori

Il componente Filtro Genitori monitora l'accesso dell'utente alle risorse Web. Lo scopo principale di Filtro Genitori è limitare l'accesso ai siti Web destinati solo a un pubblico di adulti con contenuti di tipo pornografico o che riguardano armi, abuso di sostanze stupefacenti, atti di crudeltà, violenza e così via, nonché ai siti Web che potrebbero causare distrazione e perdite di tempo (chat room, giochi) o denaro (negozi elettronici, aste).

ATTIVITÀ DI SCANSIONE ANTI-VIRUS

Oltre alla protezione costante di tutti i canali di penetrazione di programmi dannosi, è estremamente importante eseguire periodicamente la scansione anti-virus del computer. Questa operazione è necessaria per scongiurare la diffusione di programmi dannosi che non sono stati rilevati dai componenti di protezione, ad esempio perché il livello di protezione impostato era basso o per altri motivi.

In Kaspersky Anti-Virus sono incluse le attività di scansione anti-virus seguenti:

- **Scansione Personalizzata.** Scansione degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi oggetto nel file system del computer.
- **Scansione Completa.** Una scansione approfondita dell'intero sistema. Per impostazioni predefinita, vengono sottoposti a scansione gli oggetti seguenti: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di messaggi e-mail, dischi fissi, supporti di archiviazione rimovibili e unità di rete.
- **Scansione Rapida.** Scansione anti-virus degli oggetti di avvio del sistema operativo.

AGGIORNAMENTO

Per bloccare eventuali attacchi di rete, eliminare un virus o un altro programma dannoso, è necessario che Kaspersky Anti-Virus venga aggiornato regolarmente. Il componente **Aggiornamento** è stato progettato per questo scopo. Gestisce l'aggiornamento dei database dell'applicazione e dei moduli utilizzati dall'applicazione.

Il servizio di distribuzione degli aggiornamenti riduce il traffico di rete in quanto consente di salvare in una cartella locale i database e gli aggiornamenti dei moduli di programma scaricati dai server di Kaspersky Lab. Gli altri computer della rete potranno quindi accedere a tale cartella per ottenere gli aggiornamenti.

PROTEZIONE DI DATI E ATTIVITÀ ONLINE

Kaspersky Anti-Virus protegge i dati del computer dai programmi dannosi e dall'accesso non autorizzato e garantisce la sicurezza delle operazioni nella rete locale e in Internet.

Gli oggetti protetti si suddividono in tre gruppi:

- File, dati personali, parametri di accesso a risorse diverse (nomi utente e password), dati delle carte di credito e così via. La protezione di questi oggetti viene garantita da Anti-Virus File e Difesa Proattiva.
- Applicazioni installate nel computer e oggetti del sistema operativo. La protezione di questi oggetti viene fornita da Anti-Virus Posta, Anti-Virus Web, Anti-Virus IM e Difesa Proattiva.
- Attività online: utilizzo di sistemi di pagamento, protezione della posta elettronica da spam e virus e così via. La protezione di questi oggetti viene fornita da Anti-Virus Posta, Anti-Virus Web, Anti-Virus IM e Difesa Proattiva.

PROCEDURE GUIDATE E STRUMENTI

Garantire la protezione del computer è un'attività complessa che richiede una conoscenza approfondita delle funzioni del sistema operativo e dei metodi che minacciano i punti deboli. D'altro canto, la grande quantità e varietà di informazioni sulla protezione dei sistemi ne complica l'analisi e l'elaborazione.

Per facilitare la risoluzione di attività specifiche mirate a garantire la protezione del computer, nel pacchetto di Kaspersky Anti-Virus è stato incluso un insieme di procedure guidate e di strumenti.

- La Configurazione guidata del browser (vedere pagina [125](#)) analizza le impostazioni del browser Microsoft Internet Explorer e le valuta innanzitutto dal punto di vista della protezione.
- Il Ripristino guidato del sistema (vedere pagina [126](#)) elimina le tracce della presenza di oggetti malware nel sistema.
- La Pulizia guidata dati riservati (vedere pagina [127](#)) ricerca ed elimina le tracce delle attività di un utente nel sistema e nelle impostazioni del sistema operativo che consentono di raccogliere informazioni sulle attività dell'utente.
- Disco di Ripristino (vedere pagina [123](#)) è stato progettato per eseguire la scansione dei computer compatibili con le piattaforme x86 e per disinfettarli. È consigliabile utilizzare l'applicazione quando il livello di infezione è tale da reputare impossibile la disinfezione tramite applicazioni anti-virus o utilità di rimozione di malware.
- Scansione Vulnerabilità (vedere pagina [84](#)) esegue una diagnosi del computer e la ricerca delle vulnerabilità nel sistema operativo e nei programmi installati nel computer.
- Lo strumento Tastiera Virtuale (vedere pagina [122](#)) previene l'intercettazione dei dati immessi tramite tastiera.

FUNZIONALITÀ DI ASSISTENZA DEL PROGRAMMA

Kaspersky Anti-Virus comprende un insieme di funzionalità di assistenza Progettate per mantenere aggiornata la protezione del computer, espandere le funzionalità dell'applicazione e fornire un supporto per il relativo utilizzo.

File di dati e rapporti

Durante il funzionamento dell'applicazione, viene creato un rapporto per ogni componente della protezione, attività di scansione o attività di aggiornamento dell'applicazione. Tale rapporto contiene informazioni sulle attività eseguite e i risultati delle operazioni. I dati forniti consentono di conoscere nei dettagli il funzionamento dei singoli componenti di Kaspersky Anti-Virus. In caso di problemi, è possibile inviare i rapporti a Kaspersky Lab. Gli specialisti potranno approfondire la situazione e trovare una soluzione in tempi più brevi.

Kaspersky Anti-Virus sposta tutti i file sospetti in un'area di archiviazione speciale denominata *Quarantena*. I file vengono archiviati in forma crittografata per evitare di infettare il computer. È possibile eseguire la scansione anti-virus di questi oggetti, ripristinarli nella posizione iniziale, eliminarli oppure aggiungere file all'area della quarantena. Tutti i file che il completamento della scansione anti-virus dimostra essere non infetti vengono automaticamente ripristinati nel percorso iniziale.

La cartella *Backup* include le copie dei file disinfettati ed eliminati da Kaspersky Anti-Virus. Tali copie vengono create nel caso sia necessario ripristinare i file o un'immagine della rispettiva infezione. Le copie di backup dei file vengono inoltre archiviate in forma crittografata per evitare ulteriori infezioni.

È possibile ripristinare la posizione iniziale di un file dall'archivio di backup oppure eliminare una copia.

Licenza

Quando si acquista Kaspersky Anti-Virus, si stipula un contratto di licenza con Kaspersky Lab che regola l'utilizzo dell'applicazione, l'accesso agli aggiornamenti del database dell'applicazione e l'assistenza tecnica per un periodo di tempo specificato. I termini di utilizzo e le altre informazioni necessarie per la piena funzionalità dell'applicazione vengono forniti in una licenza.

Utilizzando la funzione **Licenza**, è possibile ottenere informazioni dettagliate sulla propria licenza e acquistare una nuova licenza o rinnovare quella corrente.

Assistenza tecnica

Tutti gli utenti registrati di Kaspersky Anti-Virus possono avvalersi del servizio di Assistenza tecnica. Per ulteriori dettagli sulle condizioni del servizio, utilizzare l'opzione **Assistenza**.

Seguendo i collegamenti, è possibile accedere al forum degli utenti dei prodotti Kaspersky Lab e inviare un rapporto di errore all'assistenza tecnica o un feedback sull'applicazione tramite uno speciale modulo online.

È inoltre possibile accedere ai Servizi di assistenza personalizzata e al servizio di Assistenza tecnica online. I nostri specialisti saranno sempre lieti di fornire assistenza telefonica per Kaspersky Anti-Virus.

INSTALLAZIONE DI KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus viene installato in modalità interattiva utilizzando l'installazione guidata.

Prima di iniziare l'installazione, è consigliabile chiudere tutte le applicazioni in esecuzione.

Per installare Kaspersky Anti-Virus nel computer in uso, eseguire il file di installazione, ovvero il file con estensione .exe, nel CD del prodotto.

La procedura per l'installazione di Kaspersky Anti-Virus dal file di installazione scaricato via Internet è identica a quella per l'installazione dell'applicazione dal CD.

Successivamente verrà eseguita la ricerca del pacchetto di installazione di Kaspersky Anti-Virus, ovvero il file con estensione .msi, e, se tale file viene individuato, verrà eseguita la ricerca di una nuova versione nei server di Kaspersky Lab in Internet. Se la ricerca del file non dà risultati, verrà visualizzato un messaggio in cui si propone all'utente di scaricarlo. Al completamento del download, verrà avviata l'installazione di Kaspersky Anti-Virus. Se il download viene annullato, l'installazione dell'applicazione proseguirà in modalità standard.

Il programma di installazione viene implementato come un procedura guidata Windows standard. In ogni finestra è disponibile presente un insieme di pulsanti per il controllo del processo di installazione. Di seguito vengono descritte in breve le funzioni di ciascun bottone:

- **Avanti:** accetta l'azione eseguita e accede al passaggio successivo della procedura di installazione.
- **Indietro:** torna al passaggio precedente della procedura di installazione.
- **Annulla:** annulla l'installazione.
- **Fine:** completa la procedura di installazione dell'applicazione.

Di seguito vengono illustrati in modo dettagliato tutti i passaggi della procedura di installazione.

IN QUESTA SEZIONE:

Passaggio 1. Ricerca di una versione più recente dell'applicazione.....	21
Passaggio 2. Verifica dei requisiti di sistema per l'installazione	21
Passaggio 3. Selezione del tipo di installazione	22
Passaggio 4. Visualizzazione del Contratto di licenza	22
Passaggio 5. Informativa sulla Raccolta dati per Kaspersky Security Network	22
Passaggio 6. Selezione della cartella di destinazione	23
Passaggio 7. Selezione dei componenti dell'applicazione per l'installazione	23
Passaggio 8. Utilizzo delle impostazioni dell'applicazione salvate dopo l'installazione precedente	24
Passaggio 9. Ricerca di altre applicazioni anti-virus.....	24
Passaggio 10. Preparazione finale per l'installazione.....	25
Passaggio 11. Completamento dell'installazione.....	25

PASSAGGIO 1. RICERCA DI UNA VERSIONE PIÙ RECENTE DELL'APPLICAZIONE

Prima dell'installazione, l'applicazione esegue la ricerca di una versione più recente di Kaspersky Anti-Virus nei server di aggiornamento di Kaspersky Lab.

Se non viene individuata la versione richiesta, verrà eseguita l'installazione guidata della versione corrente.

Se nei server di aggiornamento è disponibile una versione più recente di Kaspersky Anti-Virus, verrà offerta l'opportunità di scaricarla e installarla. Se l'installazione della nuova versione viene annullata, verrà eseguita l'installazione guidata della versione corrente. Se si decide di installare la versione più recente, i file di installazione verranno distribuiti nel computer e verrà avviata automaticamente l'installazione guidata.

PASSAGGIO 2. VERIFICA DEI REQUISITI DI SISTEMA PER L'INSTALLAZIONE

Prima di installare Kaspersky Anti-Virus nel computer, la procedura guidata verifica se il sistema operativo e i service pack soddisfano i requisiti del programma per l'installazione. Verifica inoltre che sia presente il software richiesto e controlla i diritti di installazione del software.

Se una condizione non è soddisfatta, viene visualizzato il messaggio di notifica corrispondente. In questo caso, prima di installare un'applicazione di Kaspersky Lab, è consigliabile installare i service pack richiesti, utilizzando il servizio Windows Update, e tutte le applicazioni necessarie.

PASSAGGIO 3. SELEZIONE DEL TIPO DI INSTALLAZIONE

Se il sistema soddisfa i requisiti di installazione e nei server di aggiornamento di Kaspersky Lab non è stato possibile trovare una versione più recente dell'applicazione, oppure se l'installazione di tale versione è stata annullata, verrà avviata l'installazione guidata della versione corrente di Kaspersky Anti-Virus.

In questa fase dell'installazione, è possibile selezionare l'opzione di installazione di Kaspersky Anti-Virus più adatta alle proprie esigenze:

- *Installazione Express.* Se si seleziona questa opzione (la casella ☒ **Installazione personalizzata** è deselezionata), l'applicazione verrà installata completamente nel computer con le impostazioni di protezione consigliate da Kaspersky Lab. Al completamento dell'installazione, verrà avviata la configurazione guidata dell'applicazione (vedere pagina [26](#)).
- *Installazione personalizzata.* In questo caso (se la casella ☒ **Installazione personalizzata** è selezionata), verrà proposto di selezionare i componenti dell'applicazione che si desidera installare e di specificare la cartella in cui verrà installata l'applicazione, nonché di attivare e configurare l'applicazione con una speciale procedura guidata.

Se si seleziona la prima opzione l'installazione guidata consentirà all'utente di visualizzare il Contratto di licenza e l'Informativa sulla raccolta dei dati di Kaspersky Security Network. Successivamente l'applicazione verrà installata nel computer.

Se si seleziona la seconda opzione, verrà richiesto di immettere o confermare determinate informazioni in ciascun passaggio dell'installazione.

Per procedere all'installazione, cliccare sul bottone **Avanti**. Per annullare l'installazione, cliccare sul bottone **Annulla**.

PASSAGGIO 4. VISUALIZZAZIONE DEL CONTRATTO DI LICENZA

In questa fase dovrebbe essere visualizzato il Contratto di licenza concluso tra l'utente e Kaspersky Lab.

Leggere attentamente il contratto e, se si accettano le condizioni, cliccare sul bottone **Accetto**. L'installazione dell'applicazione procede.

Per annullare l'installazione, cliccare sul bottone **Annulla**.

PASSAGGIO 5. INFORMATIVA SULLA RACCOLTA DATI PER KASPERSKY SECURITY NETWORK

In questo passaggio viene richiesto all'utente di partecipare al programma Kaspersky Security Network. La partecipazione a tale programma comporta l'invio di informazioni di Kaspersky Lab sulle nuove minacce rilevate nel computer in uso, dell'ID univoco assegnato al computer da Kaspersky Anti-Virus e delle informazioni di sistema. L'azienda si impegna a garantire che i dati personali non vengano divulgati.

Visualizzare la Raccolta dati per Kaspersky Security Network. Se si accettano tutte le condizioni, selezionare la casella ☒ **Accetto le condizioni di adesione al programma Kaspersky Security Network**.

Cliccare sul bottone **Avanti**. L'installazione continua.

PASSAGGIO 6. SELEZIONE DELLA CARTELLA DI DESTINAZIONE

Questo passaggio dell'installazione guidata è disponibile solo se è in esecuzione l'installazione personalizzata dell'applicazione (vedere la sezione "Passaggio 3. Selezione del tipo di installazione" a pagina [22](#)).

In questo passaggio verrà proposto all'utente di specificare la cartella in cui verrà installato Kaspersky Anti-Virus. Il percorso predefinito è:

- <unità> \ Programmi \ Kaspersky Lab \ Kaspersky Anti-Virus 2010 – per i sistemi a 32 bit.
- <unità> \ Programmi (x86) \ Kaspersky Lab \ Kaspersky Anti-Virus 2010 – per i sistemi a 64 bit.

È possibile specificare una cartella diversa cliccando sul bottone **Sfoglia** e selezionando la cartella nella finestra di selezione standard oppure immettendo il percorso nel campo di immissione corrispondente.

Tenere presente che, se si immette manualmente il percorso completo della cartella di installazione, tale percorso non deve contenere più di 200 caratteri né includere caratteri speciali.

Per procedere all'installazione, cliccare sul bottone **Avanti**.

PASSAGGIO 7. SELEZIONE DEI COMPONENTI DELL'APPLICAZIONE PER L'INSTALLAZIONE

Questo passaggio dell'installazione guidata è disponibile solo se è in esecuzione l'installazione personalizzata dell'applicazione (vedere la sezione "Passaggio 3. Selezione del tipo di installazione" a pagina [22](#)).

Se è selezionata l'installazione personalizzata, è necessario specificare i componenti di Kaspersky Anti-Virus che si desidera installare nel computer. Per impostazione predefinita, sono selezionati tutti i componenti di Kaspersky Anti-Virus, inclusi i componenti di protezione, le attività di scansione e le attività di aggiornamento.

Per decidere i componenti che non si desidera installare, visualizzare le brevi informazioni disponibili sul componente selezionando il componente nell'elenco. Le informazioni verranno visualizzate nel campo sottostante. Le informazioni includono una breve descrizione dello scopo del componente e le dimensioni di spazio su disco richieste per la relativa installazione.

Per annullare l'installazione di un componente, aprire il menu di scelta rapida sull'icona accanto al nome del componente e selezionare la voce **La funzionalità specificata diventerà non disponibile**. Se si annulla l'installazione di un componente, il computer non sarà protetto nei confronti di una serie di programmi che espongono il computer al rischio di infezione.

Per selezionare un componente per l'installazione, aprire il menu di scelta rapida sull'icona accanto al nome del componente e selezionare la voce **La funzionalità specificata sarà installata sull'unità disco fisso locale**.

Dopo aver selezionato i componenti da installare, cliccare sul bottone **Avanti**. Per tornare all'elenco predefinito di componenti da installare, cliccare sul bottone **Reimposta**.

PASSAGGIO 8. UTILIZZO DELLE IMPOSTAZIONI DELL'APPLICAZIONE SALVATE DOPO L'INSTALLAZIONE PRECEDENTE

A questo punto, l'utente potrà scegliere se utilizzare le impostazioni di protezione e i database dell'applicazione durante l'esecuzione dell'applicazione, se salvati nel computer al momento della rimozione della versione precedente di Kaspersky Anti-Virus.

Verrà ora illustrato in dettaglio come abilitare le funzionalità descritte prima.

Se nel computer è stata installata la versione precedente (build) di Kaspersky Anti-Virus e sono stati salvati i database dell'applicazione in seguito alla relativa rimozione, sarà possibile integrarli nella versione che si sta installando. A tale scopo, selezionare la casella ☒ **Database applicazione**. I database dell'applicazione inclusi nel pacchetto di installazione non verranno copiati nel computer.

Per utilizzare le impostazioni di protezione configurate in una versione precedente e salvate nel computer, selezionare la casella ☒ **Impostazioni di funzionamento dell'applicazione**.

PASSAGGIO 9. RICERCA DI ALTRE APPLICAZIONI ANTI-VIRUS

A questo punto, la procedura guidata cercherà altri programmi anti-virus, inclusi altri programmi di Kaspersky Lab, che potrebbero entrare in conflitto con Kaspersky Anti-Virus.

Se nel computer sono state rilevate altre applicazioni anti-virus, queste verranno elencate sullo schermo. Verrà chiesto di disinstallarle prima di procedere all'installazione.

È possibile selezionare la modalità di eliminazione (automatica o manuale) nell'elenco di applicazioni anti-virus individuate.

Se tra tali applicazioni è elencata la versione 2009 di un'applicazione di Kaspersky Lab, si consiglia di salvare il file di chiave utilizzato da tale applicazione durante la relativa rimozione manuale, in modo da poterlo utilizzare con una versione aggiornata dell'applicazione. Si consiglia, inoltre, di salvare gli oggetti di backup e in quarantena. Tali oggetti verranno inseriti automaticamente nella cartella degli oggetti in quarantena della versione aggiornata di Kaspersky Anti-Virus e sarà possibile continuare a utilizzarli.

Se la versione 2009 dell'applicazione viene rimossa automaticamente, le informazioni sull'attivazione verranno salvate dall'applicazione e utilizzate durante l'installazione della versione 2010.

Per procedere all'installazione, cliccare sul bottone **Avanti**.

PASSAGGIO 10. PREPARAZIONE FINALE PER L'INSTALLAZIONE

Questo passaggio completa la preparazione per l'installazione di Kaspersky Anti-Virus nel computer.

Durante l'installazione iniziale e personalizzata (vedere la sezione "Passaggio 3. Selezione del tipo di installazione" a pagina [22](#)) dell'applicazione, si consiglia di non deselezionare la casella ☒ **Proteggi il processo di installazione**. In caso di errori durante l'installazione, l'abilitazione della protezione consentirà di eseguire una procedura corretta di rollback dell'installazione. Quando si ripete l'installazione, si consiglia di deselezionare la casella.

Se l'applicazione viene installata in remoto utilizzando *Desktop remoto di Windows*, si consiglia di deselezionare la casella ☒ **Proteggi il processo di installazione**. Se si seleziona la casella, la procedura di installazione potrebbe essere eseguita in modo non corretto o non essere completata.

Per procedere all'installazione, cliccare sul bottone **Avanti**.

Durante l'installazione dei componenti di Kaspersky Anti-Virus, che rilevano il traffico di rete, le connessioni di rete correnti vengono interrotte. La maggior parte delle connessioni terminate sarà ripristinata dopo un breve intervallo di tempo.

PASSAGGIO 11. COMPLETAMENTO DELL'INSTALLAZIONE

Nella finestra **Installazione completata** sono presenti informazioni utili per il completamento dell'installazione di Kaspersky Anti-Virus nel computer in uso.

Il passaggio successivo consiste nel configurare l'applicazione per garantire la massima protezione delle informazioni memorizzate nel computer. La Configurazione guidata (vedere la sezione "Configurazione guidata dell'applicazione" a pagina [26](#)) aiuta l'utente a configurare in modo semplice e veloce Kaspersky Anti-Virus.

Cliccare sul bottone **Avanti** per passare alla configurazione dell'applicazione.

OPERAZIONI PRELIMINARI

Nella creazione di Kaspersky Anti-Virus, gli specialisti di Kaspersky Lab si sono posti l'obiettivo di fornire la configurazione ottimale dell'applicazione. Ciò consente agli utenti, indipendentemente dalle loro conoscenze in ambito informatico, di garantire in tempi rapidi e in poche mosse la protezione del computer subito dopo l'installazione.

Per maggiore comodità, è stato fatto tutto il possibile per integrare le fasi preliminari della configurazione nell'interfaccia della Configurazione guidata dell'applicazione (vedere la sezione "Configurazione guidata dell'applicazione" a pagina [26](#)) che viene avviata alla fine della procedura di installazione. Seguendo le istruzioni della procedura guidata, è possibile attivare Kaspersky Anti-Virus, configurare le impostazioni di aggiornamento, limitare l'accesso all'applicazione tramite una password e modificare altre impostazioni.

Il computer può essere infettato da malware prima che venga installato Kaspersky Anti-Virus. Per rilevare il malware, eseguire la scansione completa del computer.

A causa dell'azione del malware e di errori del sistema, le impostazioni del computer potrebbero essere danneggiate. Eseguire l'attività di scansione delle vulnerabilità (vedere la sezione "Ricerca delle vulnerabilità del computer" a pagina [31](#)) per rilevare eventuali vulnerabilità nel software installato e anomalie nelle impostazioni del sistema.

Al momento dell'installazione dell'applicazione i database inclusi nel pacchetto di installazione potrebbero inoltre diventare obsoleti. Avviare l'aggiornamento dell'applicazione, a meno che tale operazione non sia stata già eseguita utilizzando l'Installazione guidata o automaticamente subito dopo l'installazione dell'applicazione.

Il componente Anti-Spam incluso nel pacchetto di Kaspersky Anti-Virus utilizza un algoritmo di autoaddestramento per rilevare i messaggi indesiderati. Eseguire l'Addestramento guidato Anti-Spam per configurare il componente per l'utilizzo della posta.

Al termine delle azioni sopra descritte, Kaspersky Anti-Virus sarà pronto per il funzionamento. Per valutare il livello di protezione del computer, utilizzare la Gestione guidata della protezione.

IN QUESTA SEZIONE:

Configurazione guidata dell'applicazione	26
Aggiornamento dell'applicazione	30
Scansione anti-virus del computer.....	31
Ricerca delle vulnerabilità del computer	31
Gestione della licenza	32
Sottoscrizione per il rinnovo automatico della licenza	32
Partecipazione a Kaspersky Security Network	33
Gestione della protezione.....	34
Stato della protezione.....	36
Sospensione della protezione	36

CONFIGURAZIONE GUIDATA DELL'APPLICAZIONE

La Configurazione guidata dell'applicazione viene avviata al termine dell'installazione ed è progettata per consentire la configurazione delle impostazioni iniziali di Kaspersky Anti-Virus in base alle funzioni e alle attività del computer.

L'interfaccia della Configurazione guidata dell'applicazione è costituita da una serie di passaggi in finestre tra le quali è possibile spostarsi utilizzando il bottone **Indietro** e il collegamento **Avanti** o che è possibile chiudere mediante il bottone **Annulla**.

DESCRIZIONE DETTAGLIATA DEI PASSAGGI DELLA PROCEDURA GUIDATA

Passaggio 1. Attivazione dell'applicazione	27
Passaggio 2. Selezione della modalità di protezione	29
Passaggio 3. Configurazione dell'aggiornamento dell'applicazione	29
Passaggio 4. Limitazione dell'accesso all'applicazione	30
Passaggio 5. Selezione delle minacce da rilevare	30
Passaggio 6. Chiusura della procedura guidata	30

PASSAGGIO 1. ATTIVAZIONE DELL'APPLICAZIONE

La procedura di attivazione dell'applicazione consiste nella registrazione di una licenza mediante l'installazione di un file di chiave. A seconda della licenza in uso, l'applicazione determinerà i privilegi esistenti e ne calcolerà le condizioni di utilizzo.

Il file di chiave contiene informazioni di servizio necessarie per fare in modo che Kaspersky Anti-Virus sia completamente funzionale, nonché dati aggiuntivi:

- informazioni di assistenza, ovvero chi fornisce assistenza e dove può essere ottenuta;
- nome e numero del file di chiave e data di scadenza della licenza.

Per attivare l'applicazione occorre una connessione a Internet.

Per ottenere un file chiave durante l'attivazione, è necessario disporre di un codice di attivazione. Il codice di attivazione viene fornito al momento dell'acquisto dell'applicazione. L'attivazione di Kaspersky Anti-Virus prevede le opzioni seguenti:

- **Attivare la versione commerciale.** Selezionare questa opzione se è stata acquistata una versione in commercio dell'applicazione ed è stato ottenuto un codice di attivazione. È possibile utilizzare tale codice per ottenere un file di chiave che garantisca l'accesso a tutte le funzioni dell'applicazione per l'intero periodo di validità della licenza.
- **Attivare la versione di prova.** Utilizzare questa opzione di attivazione se si desidera installare la versione di prova dell'applicazione prima di procedere all'acquisto di una versione in commercio. Verrà fornito un file di chiave gratuito valido per un periodo specificato nel contratto di licenza della versione di prova.
- **Attivare successivamente.** Se si sceglie questa opzione, la fase di attivazione di Kaspersky Anti-Virus viene ignorata. L'applicazione verrà installata nel computer e sarà possibile accedere a tutte le funzioni del programma ad eccezione degli aggiornamenti (sarà disponibile un solo aggiornamento dell'applicazione subito dopo l'installazione). L'opzione **Attivare successivamente** è disponibile solo al primo avvio dell'Attivazione guidata, subito dopo l'installazione dell'applicazione.

Se Kaspersky Anti-Virus è stato installato e quindi rimosso con le informazioni sull'attivazione salvate, questo passaggio verrà ignorato. In questo caso, la Configurazione guidata riceverà automaticamente le informazioni sulla licenza esistente che verranno visualizzate nella finestra della procedura guidata (vedere a pagina [29](#)).

VEDERE ANCHE:

Attivazione della versione commerciale:.....	28
Attivazione della versione di prova	28
Completamento dell'attivazione	29

ATTIVAZIONE DELLA VERSIONE COMMERCIALE:

Se si seleziona questa opzione, l'applicazione viene attivata da un server Kaspersky Lab che richiede una connessione Internet.

L'attivazione viene eseguita immettendo un codice di attivazione inviato tramite e-mail quando si acquista Kaspersky Anti-Virus tramite Internet. Se si acquista l'applicazione in una confezione (versione definitiva), il codice di attivazione è stampato sul lato interno della copertina del disco oppure sotto lo strato protettivo dell'adesivo del lato interno della confezione del DVD.

Il codice di attivazione è una sequenza di cifre separate da trattini in quattro gruppi da cinque caratteri ciascuno e senza spazi, ad esempio 11111-11111-11111-11111. Si noti che il codice deve essere inserito in caratteri dell'alfabeto latino.

L'Attivazione guidata stabilisce una connessione con un server di attivazione di Kaspersky Lab in Internet e invia a questo il codice di attivazione in modo che possa essere verificato. Se il codice di attivazione viene accettato, l'utente riceverà un file di chiave della licenza che verrà quindi installato automaticamente. Al termine del processo di attivazione, verrà visualizzata una finestra contenente informazioni dettagliate sulla licenza acquistata.

Se si attiva la sottoscrizione, verranno rese disponibili anche informazioni sullo stato della sottoscrizione, oltre alle informazioni citate prima (vedere la sezione "Sottoscrizione per il rinnovo automatico della licenza" a pagina [32](#)).

Se il codice di attivazione non viene accettato, viene visualizzato il messaggio corrispondente. In tal caso, per ulteriori informazioni contattare il rivenditore presso il quale è stato acquistato Kaspersky Anti-Virus.

Se viene superato il numero consentito di attivazioni con il codice di attivazione specifico, viene visualizzato l'avviso corrispondente. Il processo di attivazione viene interrotto e l'applicazione consente di contattare il servizio Assistenza tecnica di Kaspersky Lab.

Se durante la connessione a un server di attivazione si sono verificati errori e non è possibile ottenere un file di chiave, contattare il Servizio di assistenza tecnica.

ATTIVAZIONE DELLA VERSIONE DI PROVA

Utilizzare questa opzione di attivazione se si desidera installare una versione di prova di Kaspersky Anti-Virus prima di procedere all'acquisto di una versione in commercio. Verrà fornito un file di chiave gratuito valido per un periodo specificato nel contratto di licenza della versione di prova. Alla scadenza della licenza di prova, non sarà possibile attivarla per la seconda volta.

Se durante la connessione a un server di attivazione si sono verificati errori e non è possibile ottenere un file di chiave, contattare il Servizio di assistenza tecnica.

COMPLETAMENTO DELL'ATTIVAZIONE

L'Attivazione guidata informa l'utente che Kaspersky Anti-Virus è stato attivato correttamente. Vengono inoltre fornite informazioni sulla licenza, ovvero il tipo (commerciale, di prova e così via), la data di scadenza e il numero di host della licenza.

Se si attiva la sottoscrizione, verranno rese disponibili informazioni sullo stato della sottoscrizione invece della data di scadenza della chiave (vedere la sezione "Sottoscrizione per il rinnovo automatico della licenza" a pagina [32](#)).

PASSAGGIO 2. SELEZIONE DELLA MODALITÀ DI PROTEZIONE

Selezionare la modalità di protezione fornita da Kaspersky Anti-Virus.

Sono disponibili due modalità:

- **Automatica.** In caso di eventi importanti, Kaspersky Anti-Virus eseguirà automaticamente l'azione consigliata dagli esperti di Kaspersky Lab. Una volta rilevata una minaccia, l'applicazione cerca di disinfettare l'oggetto e, se il tentativo non riesce, procede alla relativa eliminazione. Gli oggetti sospetti verranno ignorati senza essere elaborati. L'utente viene informato di nuovi eventi mediante messaggi a comparsa.
- **Interattiva.** In questa modalità, l'applicazione reagisce agli eventi nella maniera specificata. Quando si verifica un evento che richiede attenzione da parte dell'utente, l'applicazione visualizza notifiche (a pagina [135](#)) che consentono la selezione di un'azione.

Le notifiche sul rilevamento di un'infezione attiva verranno visualizzate a prescindere dalla modalità di protezione selezionata.

PASSAGGIO 3. CONFIGURAZIONE DELL'AGGIORNAMENTO DELL'APPLICAZIONE

Questo passaggio della Configurazione guidata dell'applicazione verrà ignorato se è stata selezionata la modalità di installazione rapida. Alle impostazioni dell'applicazione modificate in questo passaggio verranno assegnati i valori predefiniti.

L'efficacia della protezione del computer è strettamente collegata all'esecuzione di aggiornamenti periodici dei database e dei moduli del programma. In questa finestra della procedura guidata viene chiesto di selezionare la modalità di aggiornamento di Kaspersky Anti-Virus e di modificare le impostazioni di pianificazione.

- **Aggiornamenti automatici.** Kaspersky Anti-Virus verifica a intervalli specificati la disponibilità di pacchetti di aggiornamento nell'origine degli aggiornamenti. La frequenza della scansione può essere aumentata durante le epidemie e ridotta nei periodi più tranquilli. I nuovi aggiornamenti rilevati vengono scaricati e installati nel computer. Questa è la modalità predefinita.
- **Aggiornamenti pianificati** (l'intervallo di tempo può cambiare in base alle impostazioni della pianificazione). Gli aggiornamenti vengono eseguiti automaticamente in base alla pianificazione creata. Le proprietà di pianificazione possono essere modificate nella finestra visualizzata cliccando sul pulsante **Impostazioni**.
- **Aggiornamenti manuali.** Se si seleziona questa opzione, gli aggiornamenti verranno eseguiti manualmente.

Si noti che i database ed i moduli dell'applicazione in dotazione con il pacchetto di installazione potrebbero essere obsoleti al momento dell'installazione di Kaspersky Anti-Virus. È pertanto consigliabile scaricare gli aggiornamenti più recenti di Kaspersky Anti-Virus. Per farlo, cliccare su **Aggiorna ora**. Gli aggiornamenti necessari verranno scaricati dai server degli aggiornamenti e installati nel computer.

Se i database inclusi nel pacchetto di installazione sono obsoleti, le dimensioni del pacchetto di aggiornamento possono essere piuttosto grandi e aumentare ulteriormente il traffico in Internet (fino a diverse decine di MB).

Se si desidera passare alla modifica delle impostazioni di aggiornamento (selezionare la risorsa da cui verranno scaricati gli aggiornamenti, l'account utente utilizzato per eseguire il processo di aggiornamento e abilitare il servizio di distribuzione degli aggiornamenti in un'origine locale), cliccare sul bottone **Impostazioni** (vedere la sezione "Aggiornamento" a pagina [88](#)).

PASSAGGIO 4. LIMITAZIONE DELL'ACCESSO ALL'APPLICAZIONE

Questo passaggio della Configurazione guidata di Kaspersky Anti-Virus verrà ignorato se è stata selezionata la modalità di installazione rapida. Alle impostazioni dell'applicazione modificate in questo passaggio verranno assegnati i valori predefiniti.

Poiché un personal computer può essere usato da più persone, non tutte necessariamente esperte, e poiché i programmi dannosi possono disabilitare la protezione, è possibile proteggere con password l'accesso all'applicazione Kaspersky Anti-Virus. L'utilizzo di una password consente di proteggere l'applicazione da tentativi non autorizzati di disabilitare la protezione o di modificare le impostazioni di Kaspersky Anti-Virus.

Per abilitare la protezione tramite password, selezionare la casella ☒ **Abilita la protezione tramite password** e compilare i campi **Nuova password** e **Conferma la nuova password**.

Specificare l'area alla quale si intende applicare la protezione tramite password selezionando una delle opzioni seguenti:

- ☒ **Configurazione delle impostazioni dell'applicazione:** la password verrà richiesta per salvare le modifiche alle impostazioni di Kaspersky Anti-Virus.
- ☒ **Terminazione dell'applicazione:** la password verrà richiesta per chiudere l'applicazione.

PASSAGGIO 5. SELEZIONE DELLE MINACCE DA RILEVARE

Questo passaggio della Configurazione guidata dell'applicazione verrà ignorato se è stata selezionata la modalità di installazione rapida. Alle impostazioni dell'applicazione modificate in questo passaggio verranno assegnati i valori predefiniti.

In questo passaggio è possibile selezionare le categorie di minacce da rilevare mediante Kaspersky Anti-Virus. L'applicazione rileva sempre i programmi in grado di danneggiare il computer, inclusi virus, worm e Trojan.

PASSAGGIO 6. CHIUSURA DELLA PROCEDURA GUIDATA

L'ultima finestra della procedura guidata informa l'utente del completamento dell'installazione dell'applicazione. Per iniziare a lavorare con Kaspersky Anti-Virus, verificare che la casella ☒ **Avvia Kaspersky Anti-Virus** sia selezionata e cliccare sul bottone **Fine**.

AGGIORNAMENTO DELL'APPLICAZIONE

Per aggiornare Kaspersky Anti-Virus, è necessario disporre di una connessione a Internet.

Il pacchetto di installazione di Kaspersky Anti-Virus include i database che contengono firme delle minacce. Tali database potrebbero essere già obsoleti al momento dell'installazione di Kaspersky Anti-Virus in quanto insieme ai moduli dell'applicazione essi vengono aggiornati regolarmente da Kaspersky Lab.

Quando è attiva la Configurazione guidata dell'applicazione, è possibile selezionare la modalità di avvio dell'aggiornamento (vedere la sezione "Passaggio 3. Configurazione dell'aggiornamento dell'applicazione" a pagina [29](#)). Per impostazione predefinita, Kaspersky Anti-Virus controlla automaticamente la presenza di nuovi aggiornamenti sui server degli aggiornamenti di Kaspersky Lab. Se il server contiene un nuovo insieme di aggiornamenti, Kaspersky Anti-Virus li scaricherà e li installerà automaticamente.

Se i database inclusi nel pacchetto di installazione sono obsoleti, le dimensioni del pacchetto di aggiornamento possono essere piuttosto grandi e aumentare ulteriormente il traffico in Internet (fino a diverse decine di MB).

Per garantire una protezione completa del computer, si consiglia di aggiornare Kaspersky Anti-Virus immediatamente dopo l'installazione.

➡ *Per aggiornare Kaspersky Anti-Virus autonomamente, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Scegliere il bottone **Aggiorna**.

SCANSIONE ANTI-VIRUS DEL COMPUTER

Poiché gli sviluppatori di malware fanno tutto il possibile per nascondere le azioni dei loro programmi, è facile non accorgersi della presenza di tali applicazioni dannose nel computer.

Una volta installato nel computer, Kaspersky Anti-Virus esegue automaticamente l'attività di **Scansione Rapida**. Questa attività consiste nel cercare e neutralizzare i programmi nocivi negli oggetti caricati all'avvio del sistema.

Gli specialisti di Kaspersky Lab consigliano inoltre di eseguire l'attività di **Scansione Completa**.

➡ *Per avviare un'attività di scansione anti-virus, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Cliccare sul bottone **Avvia Scansione Completa** per avviare la scansione.

RICERCA DELLE VULNERABILITÀ DEL COMPUTER

Le impostazioni del sistema operativo possono danneggiarsi in seguito a errori del sistema o attività eseguite da programmi dannosi. Le applicazioni utente installate nel computer possono inoltre presentare vulnerabilità utilizzabili dagli intrusi allo scopo di danneggiare il computer.

Per rilevare ed eliminare tali problemi, è consigliabile avviare l'attività *Scansione Vulnerabilità* (vedere pagina [84](#)) dopo aver installato l'applicazione. Durante l'esecuzione di tale attività vengono ricercate le vulnerabilità nelle applicazioni installate, nonché i danni e le anomalie nelle impostazioni del browser e del sistema operativo.

➡ *Per avviare l'attività Scansione Vulnerabilità:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Cliccare sul bottone **Apri la finestra della Scansione Vulnerabilità**.
4. Nella finestra visualizzata, cliccare sul bottone **Avvia Scansione Vulnerabilità**.

GESTIONE DELLA LICENZA

Per poter funzionare, Kaspersky Anti-Virus richiede un file di chiave. Utilizzando il codice di attivazione ottenuto all'atto dell'acquisto dell'applicazione viene fornito un file di chiave che garantisce il diritto di utilizzo dell'applicazione dalla data di attivazione. Il file di chiave contiene informazioni sulla licenza, quali il tipo, la data di scadenza e il numero di host.

A meno che non sia stata attivata una versione di prova, se non si dispone di un file di chiave, Kaspersky Anti-Virus viene eseguito nella modalità che consente di scaricare un solo aggiornamento, ma non gli aggiornamenti successivi.

Al termine del periodo di prova, la versione di prova di Kaspersky Anti-Virus attivata non funziona più.

Quando la licenza commerciale scade, l'applicazione continuerà a funzionare, ma non sarà possibile aggiornare i database. Resta comunque possibile eseguire la scansione del computer per identificare la presenza di eventuali virus e utilizzare i componenti di protezione, ma solo attraverso i database aggiornati fino alla scadenza della licenza. Questo significa che la protezione dai virus diffusi dopo la scadenza della licenza dell'applicazione non potrà essere garantita.

Per evitare di infettare il computer con nuovi virus, si consiglia di estendere la licenza di Kaspersky Anti-Virus. Due settimane prima della scadenza della licenza, l'applicazione invierà un messaggio di notifica che apparirà per un determinato periodo a ogni avvio dell'applicazione.

Informazioni sulla licenza attualmente in uso sono visualizzate nella finestra **Gestione delle licenze**: il tipo (commerciale, commerciale con abbonamento, commerciale con abbonamento protezione, di prova), il numero massimo di host, la data di scadenza e il numero di giorni rimanenti. Le informazioni sulla scadenza della chiave non verranno visualizzate se è installata la licenza commerciale con sottoscrizione o la licenza commerciale con sottoscrizione di protezione (vedere la sezione "Sottoscrizione per il rinnovo automatico della licenza" a pagina [32](#)).

Per visualizzare il contratto di licenza dell'applicazione, cliccare sul bottone **Visualizza il Contratto di licenza con l'utente finale**. Per eliminare il file di chiave, cliccare sul bottone **X** a destra della licenza di cui si desidera eliminare il file di chiave. Per attivare una nuova licenza, cliccare sul bottone **Attivare una nuova licenza**.

Utilizzando il bottone **Acquista la licenza (Rinnova la licenza)**, è possibile procedere all'acquisto (rinnovo) della licenza nel negozio elettronico di Kaspersky Lab.

SOTTOSCRIZIONE PER IL RINNOVO AUTOMATICO DELLA LICENZA

La sottoscrizione consente di rinnovare la licenza automaticamente. Per attivare la sottoscrizione, è necessario un codice di attivazione che è possibile ottenere da un negozio online quando si acquista Kaspersky Anti-Virus.

Se al momento dell'attivazione della sottoscrizione si è stati già forniti di una licenza a durata limitata, questa verrà sostituita dalla licenza della sottoscrizione. Per annullare la sottoscrizione, contattare il negozio online presso il quale è stato acquistato Kaspersky Anti-Virus.

Di seguito sono indicate le opzioni utilizzate per designare lo stato della sottoscrizione:

- **Da definire.** La richiesta di attivazione della sottoscrizione non è stata elaborata. L'elaborazione della richiesta sul server richiede tempo. Kaspersky Anti-Virus funziona in modalità completamente operativa. Se dopo un determinato periodo la richiesta di sottoscrizione non risulta ancora elaborata, si riceverà una notifica al riguardo. In tal caso, i database dell'applicazione non verranno più aggiornati (per la licenza con sottoscrizione) e la protezione del computer non sarà più garantita (per la licenza con sottoscrizione alla protezione).
- **Attivata.** La sottoscrizione è stata attivata senza che sia stata fissata una scadenza oppure per un determinato periodo di tempo (la data di scadenza della sottoscrizione è stata definita).
- **Rinnovata.** La sottoscrizione è stata rinnovata senza una scadenza oppure per un determinato periodo di tempo.
- **Errore.** Si è verificato un errore durante l'aggiornamento dello stato della sottoscrizione.
- **Scaduta. Periodo di tolleranza.** La sottoscrizione è scaduta o è scaduto il periodo di tempo per il rinnovo dello stato. Se il periodo di rinnovo dello stato è scaduto, aggiornare lo stato manualmente. Se la sottoscrizione è scaduta, è possibile rinnovarla contattando il negozio online presso il quale è stato acquistato Kaspersky Anti-Virus. Prima di poter utilizzare un codice di attivazione diverso, è necessario eliminare il file di chiave per la sottoscrizione che si sta utilizzando.

- *Scaduta. Periodo di tolleranza scaduto.* La sottoscrizione è scaduta o è scaduto il periodo di tempo per il rinnovo della licenza. Contattare il fornitore della sottoscrizione per acquistare una nuova sottoscrizione oppure per rinnovare quella esistente.
- *Negata.* La sottoscrizione per il rinnovo automatico della licenza viene annullata.
- *È necessario effettuare il rinnovo.* Lo stato della sottoscrizione per qualche motivo non è stato rinnovato al momento opportuno. Utilizzare il bottone **Aggiornare stato abbonamento** per aggiornare lo stato della sottoscrizione.
- *Sospesa.* La sottoscrizione al rinnovo automatico della licenza è stata sospesa.
- *Ripresa.* La sottoscrizione è stata ripristinata.

Se sono scaduti il periodo di validità della sottoscrizione e il periodo di tolleranza concesso per il rinnovo, ovvero se lo stato della sottoscrizione è *Scaduta*, Kaspersky Anti-Virus notificherà l'informazione e interromperà i tentativi di ottenere il rinnovo automatico della licenza. Per la licenza con sottoscrizione, le funzionalità dell'applicazione verranno mantenute, ad eccezione degli aggiornamenti ai database. Per la licenza con sottoscrizione alla protezione, i database dell'applicazione non verranno aggiornati, la protezione del computer non verrà garantita e le attività di scansione non verranno eseguite.

Se la licenza non è stata rinnovata in tempo, ovvero lo stato della sottoscrizione è *È necessario effettuare il rinnovo*, ad esempio se il computer è stato spento durante tutto il periodo in cui era consentito il rinnovo della licenza, è possibile rinnovare lo stato manualmente. Fino a quando non viene effettuato il rinnovo della sottoscrizione, Kaspersky Anti-Virus non aggiorna più i database dell'applicazione (per la licenza con sottoscrizione) e non garantisce più la protezione del computer né esegue le attività di scansione (per la licenza con sottoscrizione alla protezione).

Quando si utilizza la sottoscrizione, non è possibile usare un altro codice di attivazione per rinnovare la licenza. Questa opzione sarà disponibile solo dopo la scadenza della sottoscrizione, ovvero quando lo stato della sottoscrizione è *Scaduta*. Per rinnovare la licenza, verrà concesso un periodo di tolleranza durante il quale verranno mantenute le funzionalità dell'applicazione.

Quando si utilizza la sottoscrizione e si reinstalla l'applicazione nel computer, è necessario riattivare il prodotto manualmente utilizzando il codice di attivazione ottenuto all'acquisto dell'applicazione.

L'insieme di azioni che è possibile eseguire sulla sottoscrizione può variare a seconda del fornitore della sottoscrizione. Il periodo di tolleranza in cui è possibile rinnovare la licenza non verrà concesso per impostazione predefinita.

PARTECIPAZIONE A KASPERSKY SECURITY NETWORK

In tutto il mondo appaiono quotidianamente numerose nuove minacce. Per facilitare la raccolta di statistiche sui nuovi tipi di minaccia e sulle relative origini, nonché sviluppare i metodi da utilizzare per eliminarle, Kaspersky Lab invita gli utenti a utilizzare il servizio Kaspersky Security Network.

L'utilizzo di Kaspersky Security Network implica l'invio delle seguenti informazioni a Kaspersky Lab:

- Un identificatore univoco assegnato al computer da Kaspersky Anti-Virus, che caratterizza le impostazioni hardware del computer e non contiene informazioni.
- Informazioni sulle minacce identificate dai componenti dell'applicazione. La struttura e il contenuto delle informazioni dipendono dal tipo di minaccia rilevata.
- Informazioni sul sistema: versione del sistema operativo, service pack installati, servizi e driver scaricati, versioni del browser e del client di posta elettronica, estensioni del browser, numero di versione dell'applicazione Kaspersky Lab installata.

Kaspersky Security Network raccoglie inoltre statistiche avanzate, tra cui informazioni relative a:

- file eseguibili e applicazioni firmate scaricate sul computer;
- applicazioni in esecuzione sul computer.

Le informazioni statistiche vengono inviate una volta completato l'aggiornamento dell'applicazione.

Kaspersky Lab garantisce che Kaspersky Security Network non raccoglie né distribuisce i dati personali degli utenti.

➡ Per configurare le impostazioni di invio delle statistiche:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Selezionare la sezione **Feedback** nella parte sinistra della finestra.
3. Selezionare la casella ☒ **Accetto di partecipare al programma Kaspersky Security Network** per confermare la partecipazione al programma.

GESTIONE DELLA PROTEZIONE

Lo stato di protezione del computer segnala problemi relativi alla protezione del computer (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [40](#)), indicati da un cambiamento di colore dell'icona dello stato di protezione e del pannello sul quale si trova tale icona. Se il sistema di protezione presenta problemi, si consiglia di risolverli immediatamente.

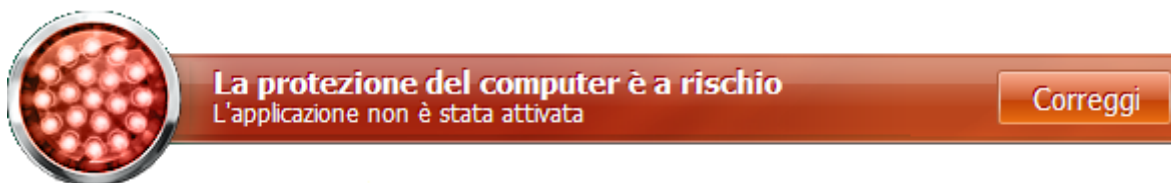


Figura 1. Stato attuale della protezione del computer

È possibile visualizzare l'elenco di problemi che si sono verificati, la relativa descrizione e i possibili rimedi nella scheda **Stato** (vedere la figura che segue). Per selezionarla, cliccare sull'icona di stato o sul pannello sul quale si trova (vedere la figura precedente).

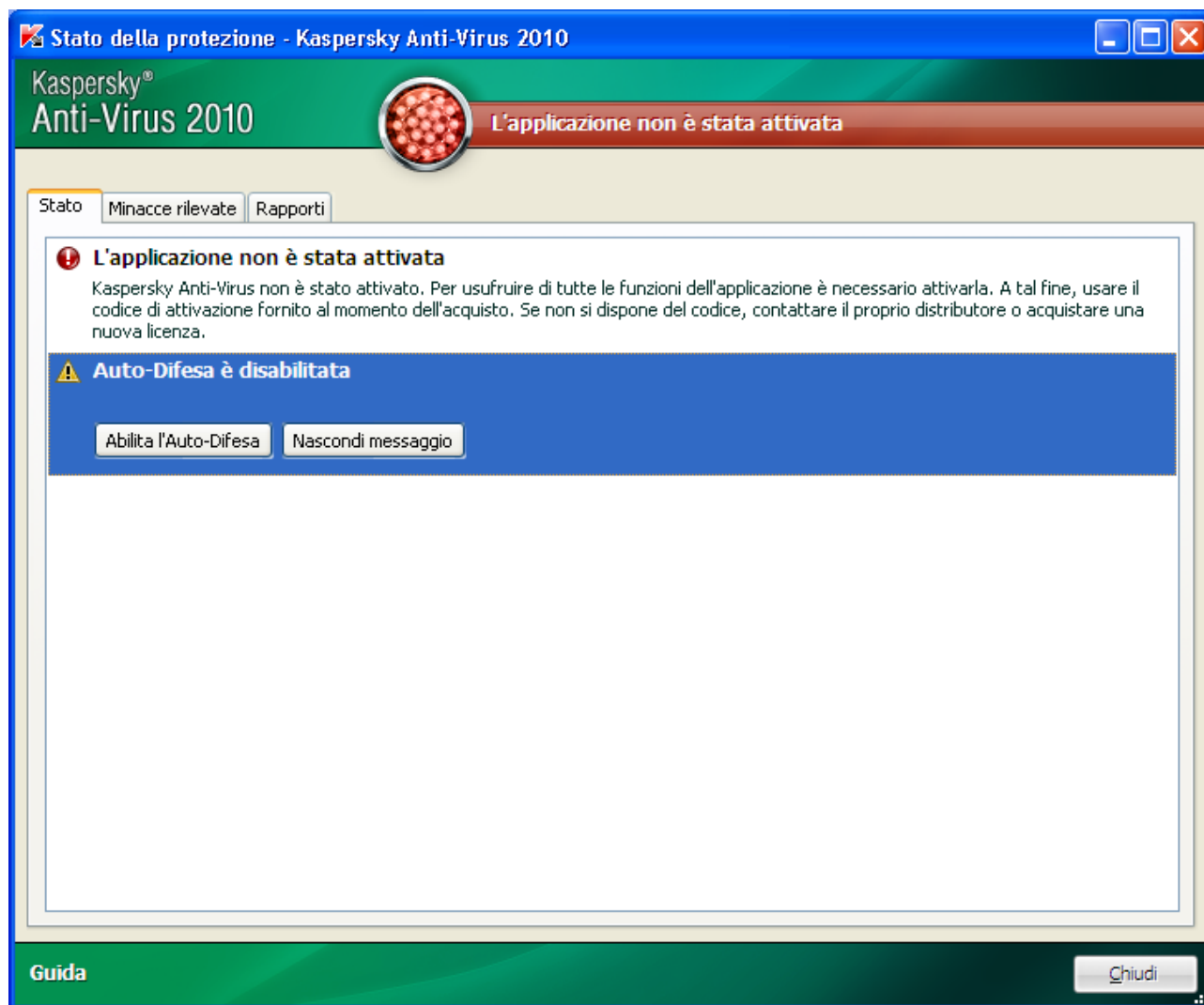


Figura 2. Risoluzione dei problemi di protezione

La scheda mostra l'elenco dei problemi correnti. I problemi vengono ordinati in base al livello di criticità: innanzitutto i problemi più critici, ovvero quelli visualizzati con l'icona di stato rossa, quindi quelli meno importanti, ovvero con l'icona di stato gialla, infine i messaggi informativi. Per ciascun problema viene fornita una descrizione dettagliata e sono disponibili le seguenti azioni:

- **Eliminazione immediata.** Con i pulsanti corrispondenti, è possibile passare alla risoluzione del problema, che è l'azione consigliata.
- **Rimanda l'eliminazione.** Se l'eliminazione immediata del problema non è possibile, è possibile ignorare questa azione ed eseguirla più tardi. A tale scopo, premere il bottone **Nascondi messaggio**.

Si noti che questa opzione non è disponibile per i problemi più seri. Tali problemi comprendono ad esempio gli oggetti dannosi non disinfettati, il blocco di uno o più componenti o il danneggiamento dei file di programma.

Per visualizzare nuovamente i messaggi nascosti nell'elenco generale, selezionare la casella ☒ **Mostra messaggi nascosti**.

STATO DELLA PROTEZIONE

Le prestazioni dei componenti di Kaspersky Anti-Virus o delle attività di scansione anti-virus vengono registrate nel rapporto contenente informazioni di riepilogo sullo stato di protezione del computer. Da qui è possibile controllare quanti oggetti pericolosi e sospetti sono stati rilevati dall'applicazione, quali sono stati disinfettati, eliminati o messi in quarantena.

Il rilevamento di un oggetto pericoloso da parte dell'applicazione viene notificato dallo stato di protezione del computer (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [40](#)) attraverso la modifica del colore dell'icona di stato e del pannello in cui si trova. Se vengono rilevati oggetti pericolosi, il colore dell'icona e del pannello diventa rosso. In questo caso, è necessario eliminare immediatamente tutte le minacce.

➤ *Per visualizzare informazioni sullo stato di protezione del computer:*

1. Aprire la finestra principale dell'applicazione.
2. Cliccare sul collegamento **Rapporti**.

➤ *Per eliminare i problemi di protezione del computer:*

1. Aprire la finestra principale dell'applicazione.
2. Cliccare sul collegamento **Rapporti**.
3. Eseguire le azioni richieste nella scheda **Stato** della finestra che viene visualizzata. Per visualizzare nuovamente i messaggi nascosti nell'elenco generale, selezionare la casella ☒ **Mostra messaggi nascosti**.

➤ *Per eseguire un'azione su un oggetto rilevato:*

1. Aprire la finestra principale dell'applicazione.
2. Cliccare sul collegamento **Rapporti**.
3. Nella finestra che viene visualizzata, scheda **Minacce rilevate**, selezionare nell'elenco quello richiesto e cliccare su di esso con il pulsante destro del mouse per aprire il menu di scelta rapida.
4. Selezionare l'azione richiesta nel menu che viene visualizzato.

➤ *Per visualizzare il rapporto sul funzionamento del componente di protezione:*

1. Aprire la finestra principale dell'applicazione.
2. Cliccare sul collegamento **Rapporti**.
3. Nella finestra visualizzata selezionare la scheda **Rapporti**.

SOSPENSIONE DELLA PROTEZIONE

Sospendere la protezione significa disabilitare temporaneamente tutti i componenti di protezione per un determinato periodo di tempo.

In seguito alla sospensione temporanea della protezione, tutti i componenti di protezione risulteranno sospesi, come indicato da:

- icona dell'applicazione inattiva (in grigio) (vedere la sezione "Icona dell'area di notifica a pagina [38](#)) nell'area della barra delle applicazioni.
- colore rosso dell'icona di stato e del pannello della finestra principale dell'applicazione.

Se durante la sospensione della protezione sono state stabilite connessioni di rete, verrà visualizzata una notifica sull'interruzione di tali connessioni.

➡ *Per sospendere la protezione del computer:*

1. Nel menu di scelta rapida dell'applicazione (vedere la sezione "Menu di scelta rapida" a pagina [39](#)), selezionare la voce **Sospensione della protezione**.
2. Nella finestra **Sospensione della protezione** visualizzata, selezionare l'intervallo di tempo dopo il quale riprendere la protezione:
 - **Sospendi per <intervallo di tempo>** – la protezione verrà abilitata dopo l'intervallo di tempo specificato. Utilizzare il menu a discesa per selezionare il valore dell'intervallo di tempo.
 - **Sospendi fino al riavvio** – la protezione verrà abilitata dopo il riavvio dell'applicazione o del sistema (a condizione che Kaspersky Anti-Virus sia impostato per l'avvio automatico).
 - **Sospendi** – la protezione verrà abilitata solo dopo il relativo avvio manuale. Per abilitare la protezione, selezionare **Riprendi la protezione** dal menu di scelta rapida dell'applicazione.

INTERFACCIA DELL'APPLICAZIONE

Kaspersky Anti-Virus presenta un'interfaccia di facile utilizzo. In questa sezione ne vengono descritte dettagliatamente le caratteristiche principali.

Kaspersky Anti-Virus include plug-in integrati in Microsoft Office Outlook, The Bat!, Microsoft Internet Explorer, Microsoft Windows Explorer. Tali plug-in estendono le funzionalità di questi programmi in quanto consentono di configurare i componenti dell'applicazione dall'interfaccia.

IN QUESTA SEZIONE:

Icona dell'area di notifica	38
Menu di scelta rapida	39
Finestra principale di Kaspersky Anti-Virus	40
Notifiche	41
Finestra delle impostazioni dell'applicazione	42

ICONA DELL'AREA DI NOTIFICA

Subito dopo aver installato l'applicazione, la relativa icona viene visualizzata nell'area di notifica della barra delle applicazioni di Microsoft Windows.

Questa icona è un indicatore del funzionamento dell'applicazione. Riflette inoltre lo stato della protezione e visualizza numerose funzioni di base eseguite dall'applicazione.

Se l'icona è attiva  (colorata), la protezione è abilitata o alcuni dei rispettivi componenti sono in esecuzione. Se l'icona è inattiva , tutti i componenti di protezione sono disabilitati.

L'icona dell'applicazione cambia in funzione dell'operazione eseguita:

-  – la posta elettronica è sottoposta a scansione;
-  – il traffico web è sottoposto a scansione;
-  – è in corso l'aggiornamento ai database e ai moduli dell'applicazione;
-  – per applicare gli aggiornamenti, è necessario riavviare il computer;
-  – si è verificato un errore nel funzionamento di alcuni componenti dell'applicazione.

L'icona consente inoltre di accedere ai componenti di base dell'interfaccia dell'applicazione: menu di scelta rapida (vedere la sezione "Menu di scelta rapida" a pagina [39](#)) e finestra principale (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [40](#)).

Per aprire il menu di scelta rapida, cliccare con il pulsante destro del mouse sull'icona dell'applicazione.

Cliccare sull'icona dell'applicazione per aprire la finestra principale di Kaspersky Anti-Virus.

Se sono disponibili notizie da Kaspersky Lab, verrà visualizzata l'icona  nell'area di notifica della barra delle applicazioni di Microsoft Windows. È possibile aprire il testo cliccando due volte sull'icona corrispondente.

MENU DI SCELTA RAPIDA

È possibile eseguire attività di protezione di base dal menu di scelta rapida, che contiene le voci seguenti:

- **Aggiorna:** avvia l'aggiornamento dei database e dei moduli dell'applicazione ed installa gli aggiornamenti nel computer.
- **Scansione Completa:** avvia una scansione completa del computer per individuare eventuali oggetti malware. Durante l'operazione vengono esaminati gli oggetti di tutte le unità, inclusi i supporti rimovibili.
- **Scansione Anti-Virus:** seleziona gli oggetti e avvia la relativa scansione antivirus. Per impostazione predefinita, l'elenco contiene diversi oggetti, tra i quali la cartella **Documenti** e le caselle di posta. È possibile ampliare l'elenco, selezionare altri oggetti per la scansione e avviare la scansione anti-virus.
- **Tastiera Virtuale:** passa alla tastiera virtuale.
- **Kaspersky Anti-Virus:** apre la finestra principale del programma (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [40](#)).
- **Impostazioni:** visualizza e configura le impostazioni dell'applicazione.
- **Attiva l'applicazione:** consente di accedere all'attivazione di Kaspersky Anti-Virus. Per ottenere lo stato di un utente registrato, è necessario attivare il programma. Questa voce di menu è disponibile solo se l'applicazione non è attivata.
- **Informazioni su:** visualizza una finestra con le informazioni sull'applicazione.
- **Sospendi della protezione / Riprendi la protezione:** disabilita o abilita temporaneamente i componenti di protezione in tempo reale. Questa voce di menu non ha effetto sull'esecuzione della scansione anti-virus o sugli aggiornamenti dell'applicazione.
- **Esci:** chiude Kaspersky Anti-Virus (quando viene selezionata questa opzione, l'applicazione viene scaricata dalla RAM del computer).



Figura 3. Menu di scelta rapida

Se è in corso un'attività di scansione anti-virus mentre si apre il menu di scelta rapida, quest'ultimo ne visualizza il nome e lo stato di avanzamento (percentuale completata). Selezionando l'attività, è possibile passare alla finestra principale contenente un rapporto sui risultati correnti della relativa esecuzione.

FINESTRA PRINCIPALE DI KASPERSKY ANTI-VIRUS

La finestra principale dell'applicazione può essere divisa in tre parti:

- La parte superiore della finestra indica l'attuale stato di protezione del computer.

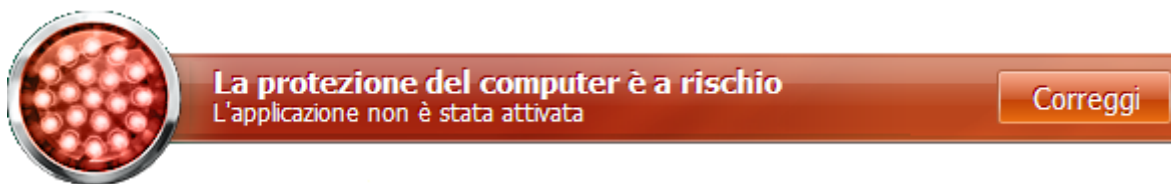


Figura 4. Stato attuale della protezione del computer

Sono disponibili tre possibili stati di protezione: ciascuno di essi è indicato da un determinato colore, analogamente ad un semaforo. Il verde indica che la protezione del computer è di livello adeguato, il giallo ed il rosso evidenziano la presenza di minacce alla protezione. Oltre ai programmi dannosi, le minacce comprendono il mancato aggiornamento del database dell'applicazione obsoleti, la disabilitazione di componenti di protezione e la selezione di impostazioni di protezione minime.

Le minacce alla protezione devono essere eliminate non appena compaiono. Per informazioni dettagliate sulle minacce e su come neutralizzarle rapidamente, passare alla Gestione guidata della protezione cliccando sull'icona di stato o sul riquadro in cui si trova (vedere la figura sopra).

- La parte sinistra della finestra consente di accedere rapidamente a qualsiasi funzione dell'applicazione, incluse le attività di scansione anti-virus, di aggiornamento e così via.



Figura 5. Parte sinistra della finestra principale

- La parte destra della finestra contiene informazioni sulla funzione dell'applicazione selezionata nella parte sinistra, consente di configurare tali funzioni e offre strumenti per eseguire attività di scansione anti-virus, scaricare aggiornamenti e così via.

Stato della Protezione
Kaspersky Anti-Virus protegge il computer dai programmi dannosi e dagli accessi non autorizzati, garantendo un uso sicuro della rete.

 **File e dati personali**
Documenti, fogli di calcolo, presentazioni, accessi e password, informazioni sulle carte di credito e altro ancora.

 **Sistema e applicazioni**
File del sistema operativo e applicazioni installate nel computer.

 **Attività online**
Navigazione sui siti Web, operazioni bancarie e acquisti online, messaggi e-mail, messaggistica istantanea e social networking.

Alcuni componenti di protezione sono disponibili solo in Kaspersky Internet Security. [Dettagli...](#)

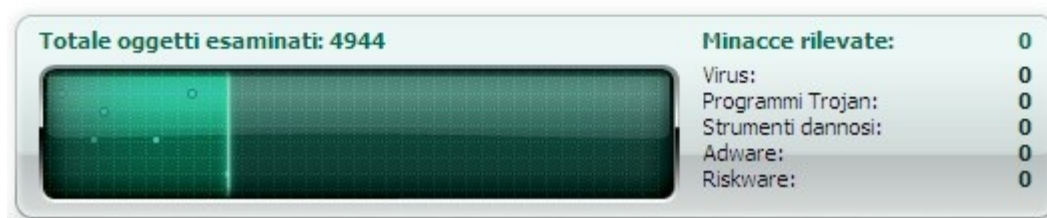


Figura 6. Parte destra della finestra principale

È inoltre possibile utilizzare i pulsanti e i collegamenti seguenti:

- **Impostazioni:** consente di aprire la finestra delle impostazioni dell'applicazione (vedere la sezione "Configurazione delle impostazioni dell'applicazione" a pagina [94](#)).
- **Quarantena:** consente di lavorare con gli oggetti in quarantena.
- **Rapporti:** consente di passare all'elenco di eventi verificatisi durante il funzionamento dell'applicazione.
- **Guida:** consente di aprire la Guida di Kaspersky Anti-Virus.
- **Pagina personale:** consente di aprire la pagina personale nel sito Web del servizio di Assistenza tecnica.
- **Assistenza:** consente di aprire la finestra contenente informazioni sul sistema e collegamenti alle risorse informative di Kaspersky Lab (sito del servizio di Assistenza tecnica, forum).
- **Licenza:** consente di attivare Kaspersky Anti-Virus estendendo il periodo di validità della licenza.

È possibile modificare l'aspetto di Kaspersky Anti-Virus creando e utilizzando diversi schemi grafici e cromatici.

NOTIFICHE

Se durante l'esecuzione di Kaspersky Anti-Virus si verificano degli eventi, sullo schermo vengono visualizzate notifiche speciali sotto forma di messaggi popup al di sopra dell'icona dell'applicazione sulla barra delle applicazioni di Microsoft Windows.

A seconda della criticità dell'evento per la protezione del computer, potrebbero essere visualizzati i tipi di notifica seguenti:

- **Allarme.** Si è verificato un evento critico, ad esempio è stato rilevato un virus o un'attività pericolosa nel sistema. È necessario decidere subito come affrontare la minaccia. Le notifiche di questo tipo sono evidenziate in rosso.
- **Attenzione.** Si è verificato un evento potenzialmente pericoloso. Ad esempio, nel sistema sono stati rilevati file potenzialmente infetti o un'attività sospetta. È necessario decidere in base al grado di pericolosità dell'evento. Le notifiche di questo tipo sono evidenziate in giallo.
- **Informazioni.** Questa notifica fornisce informazioni su eventi non critici. Le notifiche informative sono evidenziate in verde.

VEDERE ANCHE:

Notifiche [135](#)

FINESTRA DELLE IMPOSTAZIONI DELL'APPLICAZIONE

È possibile aprire la finestra delle impostazioni di Kaspersky Anti-Virus mediante la finestra principale (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [40](#)) oppure utilizzando il menu di scelta rapida (vedere la sezione "Menu di scelta rapida" a pagina [39](#)). Per farlo, cliccare sul collegamento **Impostazioni** nella parte superiore della finestra principale dell'applicazione oppure selezionare l'opzione appropriata dal menu di scelta rapida dell'applicazione.

La finestra delle impostazioni si compone di due parti:

- La parte sinistra consente di accedere alle funzioni di Kaspersky Anti-Virus, alle attività di scansione anti-virus, agli aggiornamenti e così via.
- La parte destra della finestra contiene un elenco di impostazioni relative, ad esempio, al componente e all'attività selezionati nella parte sinistra della finestra.

PROTEZIONE DEL FILE SYSTEM DEL COMPUTER

Anti-Virus File impedisce l'infezione del file system del computer. Tale strumento viene caricato all'avvio del sistema operativo ed eseguito nella RAM del computer. Esamina tutti i file che vengono aperti, salvati o eseguiti.

Per impostazione predefinita, *Anti-Virus File* esamina solo i file nuovi o modificati. Una raccolta di impostazioni, denominata livello di protezione, determina le condizioni per la scansione dei file. Se *Anti-Virus File* rileva una minaccia, eseguirà l'azione assegnata.

Il livello di protezione dei file e della memoria sul computer è determinato dalle combinazioni di impostazioni seguenti:

- quelle che determinano la creazione di un ambito di protezione;
- quelle che determinano la modalità di scansione;
- quelle che determinano la modalità di scansione dei file composti (inclusa la scansione dei file composti di grandi dimensioni);
- quelle che determinano la modalità di scansione;
- quelle che consentono di sospendere il funzionamento del componente in base alla pianificazione o durante il funzionamento delle applicazioni selezionate.

Gli specialisti di Kaspersky Lab consigliano di non configurare manualmente le impostazioni del componente *Anti-Virus File*. Nella maggior parte dei casi è sufficiente modificare il livello di protezione. Per ripristinare le impostazioni predefinite di *Anti-Virus File*, selezionare uno dei livelli di protezione.

➡ *Per modificare le impostazioni di Anti-Virus File:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Apportare le modifiche richieste alle impostazioni dell'applicazione.

IN QUESTA SEZIONE:

Algoritmo di funzionamento del componente.....	44
Modifica del livello di protezione per i file e la memoria.....	45
Modifica delle azioni da eseguire sugli oggetti rilevati	45
Creazione di un ambito di protezione	46
Utilizzo dell'analisi euristica	47
Ottimizzazione della scansione	48
Scansione di file compositi	48
Scansione di file compositi di grandi dimensioni	49
Modifica della modalità di scansione	49
Tecnologia di scansione	50
Sospensione dell'attività del componente: creazione di una pianificazione.....	50
Sospensione dell'attività del componente: creazione di un elenco di applicazioni.....	51
Ripristino delle impostazioni di protezione predefinite	52

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Il componente *Anti-Virus File* viene caricato all'avvio del sistema operativo ed eseguito nella memoria del computer. Esamina tutti i file che vengono aperti, salvati o eseguiti.

Per impostazione predefinita, Anti-Virus File esamina solo i file nuovi o modificati, ovvero i file che sono stati aggiunti o modificati dall'ultima scansione. I file vengono esaminati secondo il seguente algoritmo:

1. Il componente intercetta gli accessi a ciascun file da parte dell'utente o di qualsiasi programma.
2. Anti-Virus File esamina i database iChecker e iSwift per informazioni sul file intercettato, quindi determina se esaminare il file sulla base delle informazioni recuperate.

Durante la scansione vengono eseguite le operazioni seguenti:

1. Il file viene esaminato per verificare la presenza di virus. Gli oggetti dannosi vengono riconosciuti in base ai database di Kaspersky Anti-Virus. Il database contiene le descrizioni di tutti i programmi dannosi e le minacce attualmente noti, nonché i metodi per elaborarli.
2. Al termine dell'analisi, è possibile eseguire una delle azioni di Kaspersky Anti-Virus seguenti:
 - a. Se nel file viene rilevato codice nocivo, Anti-Virus File blocca il file, ne crea una copia di backup e tenta di disinfettarlo. Se il file viene disinfettato correttamente, diventa nuovamente disponibile. Se la disinfezione non riesce, il file viene eliminato.
 - b. Se viene rilevato codice potenzialmente dannoso, senza alcuna garanzia dell'effettiva pericolosità, il file viene comunque disinfettato e quindi inviato in un'area di memorizzazione speciale definita Quarantena.
 - c. Se nel file non viene rilevato codice dannoso, esso viene immediatamente ripristinato.

L'applicazione notificherà il rilevamento di eventuali file infetti o potenzialmente infetti. Se viene rilevato un oggetto infetto o potenzialmente infetto, sullo schermo viene visualizzato un messaggio di notifica con una richiesta di azioni ulteriori. Viene offerta la possibilità di eseguire le operazioni seguenti:

- mettere in quarantena l'oggetto, in modo da poter esaminare ed elaborare successivamente la nuova minaccia con i database aggiornati;
- eliminare l'oggetto;
- ignorare l'oggetto se si ha la certezza assoluta che non sia dannoso.

MODIFICA DEL LIVELLO DI PROTEZIONE PER I FILE E LA MEMORIA

Il livello di protezione è definito come configurazione preimpostata delle impostazioni del componente Anti-Virus File. Gli specialisti di Kaspersky Lab distinguono tre livelli di protezione. Per decidere quale livello selezionare, l'utente deve considerare le condizioni operative e la situazione corrente. Come livello di protezione è possibile selezionare una delle opzioni elencate di seguito:

- **Alto.** Impostare questo livello se si sospetta che la possibilità che il computer venga infettato sia alta.
- **Consigliato.** Questo livello garantisce un equilibrio ottimale tra efficienza e protezione ed è adatto nella maggior parte dei casi.
- **Basso.** Se si lavora in un ambiente protetto, ad esempio in una rete aziendale con una gestione della protezione centralizzata, il livello di protezione basso potrebbe essere appropriato. Questo livello può essere impostato anche quando si lavora con applicazioni che richiedono molte risorse.

Prima di abilitarlo, è consigliabile eseguire la scansione completa del computer con un livello di protezione alto.

Se nessuno dei livelli preimpostati soddisfa le proprie esigenze, è possibile configurare le impostazioni (vedere la sezione "Protezione del file system del computer" a pagina [43](#)) di Anti-Virus File autonomamente. Di conseguenza, il nome del livello di protezione verrà modificato in **Personalizzato**. Per ripristinare le impostazioni predefinite del componente, selezionare uno dei livelli di protezione preimpostati.

➡ *Per modificare il livello di protezione corrente per i file e la memoria, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Impostare il livello di protezione necessario per il componente selezionato.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

In base ai risultati della scansione, il componente Anti-Virus File assegna uno degli stati seguenti agli oggetti rilevati:

- programma dannoso, ad esempio nel caso di un *virus* o di un *Trojan*.
- *Potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che l'applicazione ha rilevato nel file una sequenza di codice di un virus sconosciuto o un codice modificato di un virus conosciuto.

Se Kaspersky Anti-Virus rileva oggetti infetti o potenzialmente infetti durante una scansione anti-virus, ne dà notifica all'utente. È necessario rispondere alla minaccia selezionando un'azione da eseguire sull'oggetto. Kaspersky Anti-Virus seleziona l'opzione **Chiedi di scegliere un'azione** come azione da eseguire su un oggetto rilevato, che rappresenta l'impostazione predefinita. È possibile modificare l'azione. Se, ad esempio, si desidera eseguire un tentativo di disinfezione per ogni oggetto rilevato ma non si desidera selezionare l'azione **Disinfetta** ogni volta che si riceve un avviso sul rilevamento di un oggetto infetto o sospetto, è necessario selezionare l'azione **Scegli l'azione automaticamente. Disinfetta**.

Prima di provare a disinfettare o eliminare un oggetto infetto, Kaspersky Anti-Virus ne crea una copia di backup per consentirne il ripristino o la disinfezione in un secondo momento.

Se si lavora in modalità automatica (vedere la sezione "Passaggio 2. Selezione della modalità di protezione" a pagina 29), Kaspersky Anti-Virus applicherà automaticamente l'azione consigliata dagli specialisti di Kaspersky Lab quando vengono rilevati oggetti pericolosi. Per gli oggetti dannosi, tale azione sarà **Disinfetta. Elimina se la disinfezione fallisce e Ignora** per gli oggetti sospetti.

➡ Per modificare l'azione specificata da eseguire sugli oggetti rilevati:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Specificare l'azione necessaria per il componente selezionato.

CREAZIONE DI UN AMBITO DI PROTEZIONE

Un ambito di protezione definisce, oltre alla posizione degli oggetti da esaminare, anche il tipo di file da esaminare. Per impostazione predefinita, Kaspersky Anti-Virus esamina solo i file potenzialmente infettabili memorizzati in qualsiasi disco rigido, unità di rete o unità rimovibile.

È possibile espandere o restringere l'ambito di protezione aggiungendo/rimuovendo gli oggetti da esaminare oppure modificando i tipi di file da esaminare. Se ad esempio si desidera esaminare solo i file *exe* eseguiti dalle unità di rete, è necessario agire con cautela per far sì che il computer non venga esposto alla minaccia di infezioni causate dalla limitazione dell'ambito di protezione.

Quando si selezionano i tipi di file, si tenga presente quanto segue:

- Alcuni formati di file (ad esempio *txt*) presentano un rischio basso di contenere codice dannoso attivabile. Altri formati, al contrario, contengono o possono contenere codice eseguibile (*exe*, *dll*, *doc*), e il rischio di attivazione di codice dannoso al loro interno è estremamente alto.
- L'intruso potrebbe inviare al computer un file con estensione *txt* che in realtà è un file eseguibile rinominato come *txt*. Selezionando l'opzione  **Esamina i file per estensione**, tale file viene ignorato dalla scansione. Se si seleziona l'opzione  **Esamina i file per formato**, Anti-Virus File analizza l'intestazione del file indipendentemente dall'estensione, rileva se si tratta di un file *.exe*, quindi esegue la scansione anti-virus.

➤ *Per modificare l'elenco di scansione degli oggetti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Generale**, sezione **Ambito della protezione**, cliccare sul collegamento **Aggiungi**.
5. Nella finestra **Scelta degli oggetti da esaminare** selezionare un oggetto e cliccare sul bottone **Aggiungi**.
6. Una volta aggiunti tutti gli oggetti richiesti, cliccare sul bottone **OK** nella finestra **Scelta degli oggetti da esaminare**.
7. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella.

➤ *Per modificare il tipo di oggetto esaminato:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Generale**, sezione **Tipi di file**, selezionare le impostazioni richieste.

UTILIZZO DELL'ANALISI EURISTICA

Gli oggetti vengono esaminati utilizzando database che contengono le descrizioni di tutti i malware noti e i metodi di disinfezione corrispondenti. Kaspersky Anti-Virus confronta ogni oggetto esaminato con le voci del database per determinare se si tratta di un oggetto dannoso e, in tal caso, identifica la classe di malware cui appartiene. Questo approccio è noto come *analisi della firma* e viene sempre utilizzato per impostazione predefinita.

Poiché ogni giorno appaiono nuovi oggetti dannosi, non tutti sono descritti nei database e possono quindi essere rilevati solo attraverso l'analisi euristica. Questo metodo presuppone l'analisi delle azioni eseguite da un oggetto all'interno del sistema. Se tali azioni sono tipiche di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto. In questo modo è possibile rilevare le nuove minacce prima ancora che queste vengano studiate dagli analisti anti-virus.

Se viene rilevato un oggetto dannoso, viene visualizzato un messaggio di notifica in cui viene richiesto di eseguire un'azione.

Inoltre, è possibile impostare il livello di dettaglio delle scansioni. Questo livello definisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e il tempo richiesto per la scansione. Maggiore è il livello di dettaglio, più risorse saranno necessarie e maggiore sarà la durata della scansione.

➤ *Per utilizzare l'analisi euristica e impostare il livello di dettaglio delle scansioni:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Prestazioni**, sezione **Metodi di scansione**, selezionare la casella ☒ **Analisi euristica** e specificare il livello di dettaglio della scansione.

OTTIMIZZAZIONE DELLA SCANSIONE

Per ridurre la durata delle scansioni e per aumentare la velocità di Kaspersky Anti-Virus, è possibile scegliere di sottoporre a scansione solo i file nuovi e i file modificati dopo l'ultima analisi. Questa modalità si estende ai file semplici e a quelli composti.

➡ *Per sottoporre a scansione solo i file nuovi e quelli modificati dall'ultima scansione:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Prestazioni**, sezione **Ottimizzazione della scansione**, selezionare la casella ☒ **Esamina solo i file nuovi e modificati**.

SCANSIONE DI FILE COMPOSITI

Un metodo comune per nascondere i virus consiste nell'incorporarli in file composti, ovvero archivi, database e così via. Per individuare i virus nascosti in questo modo, è necessario decomprimere un file composto, operazione che può ridurre in modo significativo la velocità di scansione.

I pacchetti di installazione e i file contenenti oggetti OLE vengono eseguiti all'apertura, risultando quindi più pericolosi degli archivi. Disabilitando la scansione degli archivi e abilitando la scansione di questi tipi di file, il computer viene protetto dall'esecuzione di codice dannoso e, al tempo stesso, la velocità di scansione aumenta.

Per impostazione predefinita, Kaspersky Anti-Virus esamina esclusivamente gli oggetti OLE incorporati.

➡ *Per modificare l'elenco dei file composti esaminati:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Prestazioni** della sezione **Scansione dei file composti**, selezionare le caselle ☒ relative ai tipi di file composti da sottoporre a scansione.

SCANSIONE DI FILE COMPOSITI DI GRANDI DIMENSIONI

Durante la scansione di file composti di grandi dimensioni, la decompressione preliminare può richiedere molto tempo. L'operazione può essere accelerata se la scansione dei file viene effettuata in background. Se durante l'utilizzo di questi file è stato rilevato un oggetto dannoso, viene visualizzato un messaggio di notifica.

Per accedere più rapidamente ai file composti, è possibile disabilitare la decompressione dei file la cui dimensione supera il valore specificato. Quando i file vengono estratti da un archivio, vengono sempre sottoposti a scansione.

➤ *Per abilitare la decompressione in background di file di grandi dimensioni da parte di Kaspersky Anti-Virus, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Prestazioni**, sezione **Scansione dei file composti**, cliccare sul bottone **Avanzate**.
5. Nella finestra **File composti**, selezionare la casella ☒ **Estrai i file composti in background** e specificare la dimensione di file minima nel campo sottostante.

➤ *Per disabilitare la decompressione di file di grandi dimensioni da parte di Kaspersky Anti-Virus, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Prestazioni**, sezione **Scansione dei file composti**, cliccare sul bottone **Avanzate**.
5. Nella finestra **File composti** visualizzata, selezionare la casella ☒ **Non decomprimere i file composti di grandi dimensioni** e specificare la dimensione di file nel campo adiacente.

MODIFICA DELLA MODALITÀ DI SCANSIONE

Per modalità di scansione si intende la condizione che attiva il funzionamento del componente Anti-Virus File. Per impostazione predefinita, Kaspersky Anti-Virus utilizza una modalità intelligente per determinare se l'oggetto è soggetto a scansione in base alle azioni eseguite su di esso. Ad esempio, quando si lavora con un documento Microsoft Office, il file viene sottoposto a scansione quando viene aperto per la prima e chiuso per l'ultima volta. Le operazioni intermedie che lo sovrascrivono non determinano la scansione del file.

La modalità di scansione degli oggetti può essere modificata. La selezione della modalità dipende dai file con i quali si lavora più spesso.

➤ *Per modificare la modalità di scansione degli oggetti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Avanzate**, sezione **Modalità di scansione**, selezionare la modalità richiesta.

TECNOLOGIA DI SCANSIONE

È inoltre possibile specificare le tecnologie che verranno utilizzate dal componente Anti-Virus File:

- **iChecker.** Questa tecnologia è in grado di aumentare la velocità di scansione escludendo determinati oggetti dalla scansione. Un oggetto viene escluso dalla scansione attraverso uno speciale algoritmo che tiene conto della data di rilascio del database di Kaspersky Anti-Virus, la data dell'ultima scansione dell'oggetto e le eventuali modifiche apportate alle impostazioni di scansione.

Si supponga, ad esempio, di disporre di un file archivio a cui dopo la scansione è stato assegnato lo stato *non infetto*. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se la struttura dell'archivio risulta modificata perché è stato aggiunto un nuovo oggetto oppure se le impostazioni di scansione sono state modificate o i database dell'applicazione aggiornati, il programma esaminerà nuovamente l'archivio.

iChecker presenta tuttavia delle limitazioni: non risulta efficace con file di grandi dimensioni ed è applicabile solo agli oggetti con una struttura riconosciuta dall'applicazione, ad esempio file *.exe*, *.dll*, *.lnk*, *.ttf*, *.inf*, *.sys*, *.com*, *.chm*, *.zip*, *.rar*.

- **iSwift.** Questa tecnologia è stata sviluppata a partire dalla tecnologia iChecker per i computer che utilizzano un file system di tipo NTFS. Anche la tecnologia iSwift presenta delle limitazioni: è associata a un percorso di file specifico nel file system e può essere applicata solo a oggetti in NTFS.

► Per cambiare tecnologia di scansione degli oggetti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Avanzate** della sezione **Tecnologie di scansione**, selezionare il valore di impostazione appropriato.

SOSPENSIONE DELL'ATTIVITÀ DEL COMPONENTE: CREAZIONE DI UNA PIANIFICAZIONE

Durante l'esecuzione di determinati programmi che richiedono una considerevole quantità di risorse, è possibile sospendere temporaneamente l'attività del componente Anti-Virus File, consentendo un accesso più rapido agli oggetti. Per ridurre il carico e garantire un accesso rapido agli oggetti, è possibile impostare una pianificazione per la disabilitazione del componente.



Figura 7. Creazione di una pianificazione

➡ Per configurare una pianificazione per sospendere l'attività del componente:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Avanzate** della sezione **Sospendi l'attività**, selezionare la casella ☒ **In base alla pianificazione** e cliccare sul bottone **Pianificazione**.
5. Nella finestra **Sospensione dell'attività**, specificare l'intervallo (nel formato 24 ore HH:MM) durante il quale la protezione sarà sospesa (campi **Sospendi l'attività alle** e **Riprendi l'attività alle**).

SOSPENSIONE DELL'ATTIVITÀ DEL COMPONENTE: CREAZIONE DI UN ELENCO DI APPLICAZIONI

Durante l'esecuzione di determinati programmi che richiedono una considerevole quantità di risorse, è possibile sospendere temporaneamente l'attività del componente Anti-Virus File, consentendo un accesso più rapido agli oggetti. Per diminuire il carico e garantire un rapido accesso agli oggetti, è possibile configurare le impostazioni per la disabilitazione del componente quando si utilizzano determinate applicazioni.

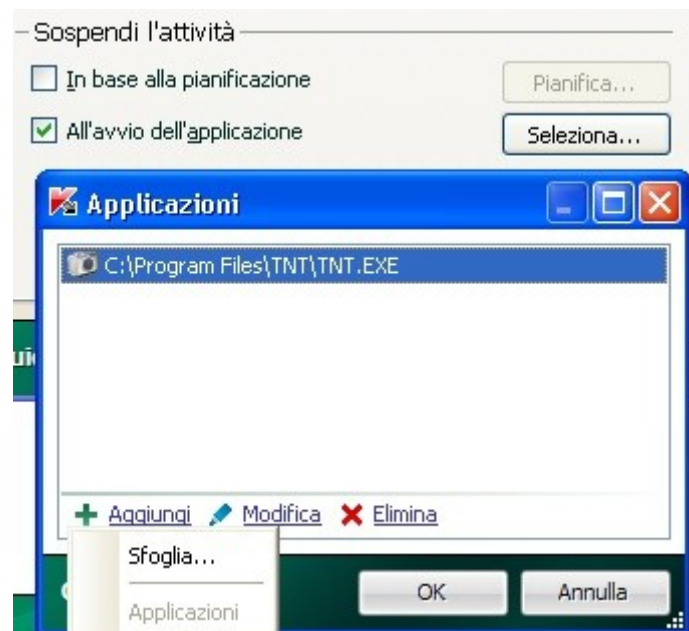


Figura 8. Creazione di un elenco di applicazioni

La configurazione della disabilitazione del componente Anti-Virus File in caso di conflitti con determinate applicazioni rappresenta una misura drastica. In caso di conflitti durante l'utilizzo del componente, contattare il servizio di assistenza tecnica di Kaspersky Lab (<http://support.kaspersky.it>). Gli specialisti dell'assistenza tecnica aiuteranno a risolvere i problemi di funzionamento di Kaspersky Anti-Virus in contemporanea con il software presente nel computer.

➡ *Per configurare la sospensione del componente mentre sono in uso le applicazioni specificate, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Avanzate** della sezione **Sospendi l'attività**, selezionare la casella ☒ **All'avvio dell'applicazione** e cliccare sul bottone **Seleziona**.
5. Nella finestra **Applicazioni**, creare un elenco di applicazioni che sospenderanno il componente durante l'esecuzione.

RIPRISTINO DELLE IMPOSTAZIONI DI PROTEZIONE PREDEFINITE

Quando si configura Anti-Virus File, è sempre possibile ripristinare le impostazioni consigliate. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Esse sono raggruppate nel livello di protezione **Consigliato**.

➡ *Per ripristinare le impostazioni predefinite relative alla protezione, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Nella sezione **Livello di protezione**, cliccare sul bottone **Livello predefinito** relativo al componente selezionato.

PROTEZIONE DELLA POSTA

Anti-Virus Posta esamina i messaggi di posta elettronica in entrata e in uscita per verificare la presenza di oggetti dannosi. Viene avviato durante il caricamento del sistema operativo, si trova nella RAM del computer ed esamina tutti i messaggi di posta ricevuti tramite i protocolli POP3, SMTP, IMAP, MAPI e NNTP.

Una raccolta di impostazioni, denominata livello di protezione, determina la modalità di scansione dei messaggi e-mail. Quando viene rilevata una minaccia, Anti-Virus Posta esegue l'azione specificata dall'utente (vedere la sezione "Modifica delle azioni da eseguire sugli oggetti rilevati" a pagina [55](#)). Le regole di scansione della posta elettronica sono definite da una serie di impostazioni. Tali regole possono essere suddivise in gruppi e determinano le funzionalità seguenti:

- flusso di posta protetto;;
- utilizzo dei metodi di analisi euristica;;
- scansione dei file compositi;;
- filtraggio dei file allegati.

Kaspersky Lab consiglia di non configurare manualmente le impostazioni di Anti-Virus Posta. Nella maggior parte dei casi è sufficiente selezionare un livello di protezione diverso. È possibile ripristinare le impostazioni predefinite di Anti-Virus Posta. A tale scopo, selezionare uno dei livelli di protezione disponibili.

► Per modificare le impostazioni di Anti-Virus Posta, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Posta**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Apportare le modifiche richieste alle impostazioni dell'applicazione.

IN QUESTA SEZIONE:

Algoritmo di funzionamento del componente.....	54
Modifica del livello di protezione dei messaggi di posta elettronica.....	54
Modifica delle azioni da eseguire sugli oggetti rilevati.....	55
Creazione di un ambito di protezione.....	56
Scansione della posta elettronica in Microsoft Office Outlook.....	57
Scansione della posta elettronica in The Bat!.....	57
Utilizzo dell'analisi euristica.....	58
Scansione di file compositi.....	58
Filtraggio degli allegati.....	59
Ripristino delle impostazioni di protezione predefinite della posta elettronica.....	59

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Kaspersky Anti-Virus include il componente che consente di eseguire la scansione della posta elettronica per rilevare la presenza di oggetti pericolosi, denominato *Anti-Virus Posta*. Tale componente viene caricato all'avvio del sistema operativo ed è sempre in esecuzione per esaminare tutta la posta elettronica sui protocolli POP3, SMTP, IMAP, MAPI e NNTP, nonché le connessioni protette (SSL) per POP3 e IMAP.

L'indicatore di funzionamento del componente è l'icona dell'applicazione nell'area di notifica della barra delle applicazioni, che ha un aspetto simile al seguente  quando viene eseguita la scansione di un messaggio e-mail.

Per impostazione predefinita, la posta viene protetta nel modo seguente:

1. Ogni messaggio di posta ricevuto o inviato dall'utente viene intercettato dal componente.
2. Il messaggio viene scomposto nelle sue parti: l'intestazione, il corpo e gli allegati.
3. Il corpo e gli allegati del messaggio (inclusi gli oggetti OLE) vengono esaminati per escludere la presenza di oggetti pericolosi. Gli oggetti dannosi vengono rilevati con i database utilizzati da Kaspersky Anti-Virus e con un algoritmo euristico. Il database contiene le descrizioni di tutti i programmi dannosi attualmente conosciuti, nonché i metodi che consentono di neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti nel database.
4. Dopo la scansione anti-virus, è possibile eseguire le azioni seguenti:
 - Se il corpo o gli allegati del messaggio contengono un codice dannoso, il componente Anti-Virus File blocca il messaggio, ne crea una copia di backup e cerca di disinfettare l'oggetto. Dopo aver completato la disinfezione, lo restituisce all'utente. Se la disinfezione non riesce, l'oggetto infetto viene eliminato dal messaggio. Dopo la scansione anti-virus, nella riga dell'oggetto del messaggio compare un testo che segnala che è in corso l'elaborazione del messaggio da parte di Kaspersky Anti-Virus.
 - Se nel corpo o in un allegato viene rilevato codice potenzialmente dannoso, la cui pericolosità non è tuttavia garantita, la parte sospetta del messaggio viene spostata in un'area di memorizzazione speciale denominata Quarantena.
 - Se all'interno del messaggio non viene individuato alcun codice dannoso, il messaggio viene reso immediatamente disponibile all'utente.

Per Microsoft Office Outlook viene fornito un modulo di estensione integrato (vedere la sezione "Scansione della posta elettronica in Microsoft Office Outlook" a pagina [57](#)) che consente di ottimizzare il client di posta.

Se si utilizza il client di posta The Bat!, Kaspersky Anti-Virus può essere utilizzato unitamente ad altre applicazioni anti-virus. In questo caso, le regole per l'elaborazione del traffico e-mail (vedere la sezione "Scansione della posta elettronica in The Bat!" a pagina [57](#)) vengono configurate direttamente in The Bat! e sostituiscono le impostazioni di protezione e-mail dell'applicazione.

Se si lavora con altri programmi di posta (inclusi Microsoft Outlook Express/Windows Mail, Mozilla Thunderbird, Eudora e Incredimail), Anti-Virus Posta esamina i messaggi sui protocolli SMTP, POP3, IMAP, e NNTP.

Si noti che quando si lavora con il client di posta Thunderbird, i messaggi di posta elettronica trasferiti attraverso IMAP non verranno sottoposti a una scansione anti-virus se vengono utilizzati filtri per il trasferimento dei messaggi dalla cartella **Posta in arrivo**.

MODIFICA DEL LIVELLO DI PROTEZIONE DEI MESSAGGI DI POSTA ELETTRONICA

Il livello di protezione è definito come configurazione preimpostata delle impostazioni del componente Anti-Virus File. Gli specialisti di Kaspersky Lab distinguono tre livelli di protezione. Per decidere quale livello selezionare, l'utente deve considerare le condizioni operative e la situazione corrente. È possibile selezionare uno dei livelli di protezione seguenti:

- **Alto.** Se si lavora in un ambiente non protetto, è consigliabile impostare il livello massimo di protezione. Un esempio di ambiente di questo tipo è rappresentato da una connessione a un servizio di posta elettronica gratuito, da una rete priva di protezione centralizzata della posta elettronica.
- **Consigliato.** Questo livello garantisce un equilibrio ottimale tra efficienza e protezione ed è adatto nella maggior parte dei casi. Rappresenta anche l'impostazione predefinita.
- **Basso.** Se si lavora in un ambiente ben protetto, è possibile utilizzare il livello di protezione basso. Un esempio di ambiente di questo tipo è rappresentato da una rete aziendale con protezione centralizzata della posta elettronica.

Se nessuno dei livelli preimpostati soddisfa le proprie esigenze, è possibile configurare le impostazioni (vedere la sezione "Protezione del file system del computer" a pagina [53](#)) di Anti-Virus Posta autonomamente. Di conseguenza, il nome del livello di protezione verrà modificato in **Personalizzato**. Per ripristinare le impostazioni predefinite del componente, selezionare uno dei livelli di protezione preimpostati.

➡ *Per modificare il livello di protezione della posta elettronica preimpostato:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Posta**.
3. Impostare il livello di protezione necessario per il componente selezionato.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Anti-Virus Posta esamina un messaggio di posta elettronica. Se la scansione indica che il messaggio o una delle sue parti (corpo, allegato) è infetto o potenzialmente infetto, le successive operazioni del componente dipendono dallo stato dell'oggetto e dall'azione selezionata.

Come risultato della scansione, Anti-Virus Posta assegna uno degli stati seguenti agli oggetti rilevati:

- programma dannoso, ad esempio nel caso di un *virus* o di un *Trojan*.
- *Potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il messaggio di posta o l'allegato contiene una sequenza di codice di un virus sconosciuto o un codice modificato di un virus conosciuto.

Se Kaspersky Anti-Virus rileva oggetti infetti o potenzialmente infetti durante la scansione della posta, ne dà notizia all'utente. È necessario rispondere alla minaccia selezionando un'azione da eseguire sull'oggetto. Kaspersky Anti-Virus seleziona l'opzione **Chiedi di scegliere un'azione** come azione da eseguire su un oggetto rilevato, che rappresenta l'impostazione predefinita. È possibile modificare l'azione. Se, ad esempio, si desidera eseguire un tentativo di disinfezione per ogni oggetto rilevato ma non si desidera selezionare l'azione **Disinfetta** ogni volta che si riceve un avviso sul rilevamento di un oggetto infetto o sospetto in un messaggio, è necessario selezionare l'azione **Scegli l'azione automaticamente. Disinfetta**.

Prima di provare a disinfettare o eliminare un oggetto infetto, Kaspersky Anti-Virus ne crea una copia di backup per consentirne il ripristino o la disinfezione in un secondo momento.

Se si lavora in modalità automatica (vedere la sezione "Passaggio 2. Selezione della modalità di protezione" a pagina [29](#)), Kaspersky Anti-Virus applicherà automaticamente l'azione consigliata dagli specialisti di Kaspersky Lab quando vengono rilevati oggetti pericolosi. Per gli oggetti dannosi, tale azione sarà **Disinfetta. Elimina se la disinfezione fallisce e Ignora** per gli oggetti sospetti.

➡ Per modificare l'azione specificata da eseguire sugli oggetti rilevati:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Posta**.
3. Specificare l'azione necessaria per il componente selezionato.

CREAZIONE DI UN AMBITO DI PROTEZIONE

Per ambito di protezione si intende il tipo di messaggi da esaminare. Per impostazione predefinita, Kaspersky Anti-Virus esamina sia i messaggi in entrata che in uscita. Se si è scelto di esaminare solo i messaggi in entrata, si consiglia di esaminare anche quelli in uscita quando Kaspersky Anti-Virus viene utilizzato per la prima volta in quanto è probabile che il computer contenga worm che potrebbero diffondersi tramite la posta elettronica. Questa misura precauzionale contribuirà a evitare situazioni spiacevoli causate spesso da invii non controllati di grandi quantità di messaggi di posta infetti provenienti dal proprio computer.

L'ambito di protezione include inoltre le impostazioni utilizzate per l'integrazione di Anti-Virus Posta nel sistema e i protocolli da esaminare. Per impostazione predefinita, il componente Anti-Virus Posta è integrato nei client di posta Microsoft Office Outlook e The Bat!.

➡ Per disabilitare la scansione della posta in uscita, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Posta**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Specificare nella finestra visualizzata i valori richiesti per le impostazioni nella scheda **Generale** della sezione **Ambito della protezione**.

➡ Per selezionare i protocolli da esaminare e le impostazioni per l'integrazione di Anti-Virus Posta nel sistema, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Posta**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Avanzate** della sezione **Connettività**, selezionare le impostazioni appropriate.

SCANSIONE DELLA POSTA ELETTRONICA IN MICROSOFT OFFICE OUTLOOK

Se si utilizza Microsoft Office Outlook come client di posta elettronica, è possibile configurare impostazioni aggiuntive per la scansione anti-virus della posta.

Quando si installa Kaspersky Anti-Virus, viene installato uno speciale plug-in in Microsoft Office Outlook che consente di configurare velocemente le impostazioni del componente Anti-Virus Posta e determinare i messaggi di posta elettronica che verranno esaminati per cercare eventuali oggetti pericolosi.

Il plug-in si presenta sotto forma di una scheda speciale denominata **Anti-Virus Posta** che si trova nel menu **Strumenti** → **Opzioni**. Questa scheda consente di specificare le modalità di scansione della posta.

➡ *Per specificare condizioni di filtraggio complesse:*

1. Aprire la finestra principale di Microsoft Office Outlook.
2. Selezionare **Strumenti** → **Opzioni** dal menu dell'applicazione.
3. Selezionare la scheda **Anti-Virus Posta** e specificare la modalità di scansione della posta richiesta.

SCANSIONE DELLA POSTA ELETTRONICA IN THE BAT!

Le azioni da intraprendere sugli oggetti di posta infetti nel client The Bat! vengono definite mediante gli strumenti del programma stesso.

Le impostazioni di Anti-Virus Posta che determinano se è necessario eseguire la scansione dei messaggi in ingresso e in uscita, le azioni da eseguire sugli oggetti pericolosi nella posta elettronica e le esclusioni da applicare, vengono ignorate. L'unica azione presa in considerazione da The Bat! è la scansione degli archivi allegati.

Le impostazioni di protezione della posta elettronica si estendono a tutti i moduli anti-virus installati nel computer che supportano The Bat!.

Tenere presente che i messaggi e-mail in entrata vengono esaminati prima da Anti-Virus Posta e solo successivamente dal plug-in del client di posta di The Bat!. Se viene individuato un oggetto dannoso, Kaspersky Anti-Virus informerà immediatamente l'utente. Se si seleziona l'azione **Disinfetta (Elimina)** nella finestra di notifica di Anti-Virus Posta, le azioni mirate all'eliminazione della minaccia verranno eseguite da questo componente. Se si seleziona l'azione **Ignora** nella finestra di notifica, l'oggetto verrà disinfettato dal plug-in di The Bat!. Quando si inviano messaggi e-mail, la scansione viene eseguita prima dal plug-in e quindi da Anti-Virus Posta.

È necessario decidere:

- quale flusso di messaggi di posta elettronica sarà esaminato (in entrata in uscita).
- In che momento gli oggetti della posta elettronica saranno analizzati (all'apertura di un messaggio o prima di salvarlo su disco);
- le azioni intraprese dal client di posta quando nei messaggi di posta elettronica vengono rilevati oggetti pericolosi. È ad esempio possibile selezionare:
 - **Tenta di disinfettare le parti infette:** se questa opzione è selezionata, si tenterà di disinfettare l'oggetto infetto. Se non è possibile disinfettarlo, resterà nel messaggio.
 - **Elimina parti infette:** se questa opzione è selezionata, l'oggetto pericoloso presente nel messaggio viene eliminato indipendentemente dal fatto che sia infetto o sospetto.

Per impostazione predefinita, The Bat! trasferisce tutti gli oggetti di posta infetti nella cartella Quarantena senza tentare di disinfettarli.

The Bat! non assegna intestazioni speciali ai messaggi contenenti oggetti pericolosi.

➤ *Per impostare le regole di protezione della posta in The Bat!:*

1. Aprire la finestra principale di The Bat!.
2. Selezionare **Settings (Impostazioni)** dal menu **Properties (Proprietà)** del client di posta.
3. Selezionare **Virus protection (Protezione anti-virus)** nella struttura ad albero delle impostazioni.

UTILIZZO DELL'ANALISI EURISTICA

Il metodo euristico implica l'analisi delle attività eseguite dall'oggetto nel sistema. Se tali azioni sono tipiche di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto. In questo modo è possibile rilevare le nuove minacce prima che queste vengano studiate dagli analisti anti-virus. L'analisi euristica è abilitata per impostazione predefinita.

Kaspersky Anti-Virus informa l'utente della presenza di un oggetto nocivo rilevato in un messaggio. È necessario rispondere alla notifica elaborando ulteriormente il messaggio.

È inoltre possibile impostare il livello di dettaglio per le scansioni: **Superficiale**, **Media** o **Approfondita**, spostando il cursore nella posizione selezionata.

➤ *Per abilitare/disabilitare l'analisi euristica e impostare il livello di dettaglio della scansione, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Posta**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, scheda **Generale**, sezione **Metodi di scansione**, selezionare/deselezionare la casella ☒ **Analisi euristica** e specificare il livello di dettaglio della scansione.

SCANSIONE DI FILE COMPOSITI

La selezione della modalità di scansione dei file composti influisce sulle prestazioni di Kaspersky Anti-Virus. È possibile abilitare o disabilitare la scansione degli archivi allegati e limitare le dimensioni massime degli archivi da esaminare.

➤ *Per configurare le impostazioni di scansione dei file composti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Posta**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Generale**, selezionare la modalità di scansione dei file composti.

FILTRAGGIO DEGLI ALLEGATI

È possibile configurare le condizioni di filtraggio per gli allegati di posta elettronica. L'uso del filtro consente di aumentare la protezione del computer, in quanto nella maggior parte dei casi i programmi dannosi si diffondono attraverso l'invio di allegati. Rinominando o eliminando determinati tipi di allegato, è possibile proteggere il computer da potenziali pericoli, ad esempio l'apertura automatica degli allegati alla ricezione di un messaggio.

Se il computer non è protetto da alcun software di rete locale e se si accede a Internet direttamente senza un server proxy o un firewall, si consiglia di non disabilitare la scansione degli archivi allegati.

➡ *Per configurare le impostazioni di filtraggio degli allegati:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Posta**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra visualizzata, nella scheda **Filtro allegati**, specificare le condizioni di filtraggio per gli allegati di posta elettronica. Selezionando una delle ultime due modalità l'elenco di tipi di file diventa attivo e consente di specificare i tipi richiesti o di aggiungere una maschera per la selezione di un nuovo tipo.

Se è necessario aggiungere una maschera di un nuovo tipo, cliccare sul collegamento **Aggiungi** e immettere i dati richiesti in **Maschera per il nome del file** nella finestra visualizzata.

RIPRISTINO DELLE IMPOSTAZIONI DI PROTEZIONE PREDEFINITE DELLA POSTA ELETTRONICA

Quando si configura Anti-Virus Posta, è sempre possibile ripristinarne le impostazioni consigliate. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Esse sono raggruppate nel livello di protezione **Consigliato**.

➡ *Per ripristinare le impostazioni predefinite relative alla posta, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Posta**.
3. Nella sezione **Livello di protezione**, cliccare sul bottone **Livello predefinito** relativo al componente selezionato.

PROTEZIONE DEL TRAFFICO WEB

Ogni volta che si usa Internet, si espongono le informazioni memorizzate nel computer al rischio di infezione da parte di programmi pericolosi. Tali programmi possono accedere al computer durante il download di programmi gratuiti o la navigazione in siti ritenuti sicuri che di recente hanno subito attacchi di rete. Inoltre, i worm di rete possono accedere al computer ancora prima dell'apertura di una pagina Web o del download di un file, in quanto è sufficiente che il computer sia collegato a Internet.

Il componente *Anti-Virus Web* è progettato per garantire la protezione durante l'utilizzo di Internet. Esso protegge il computer dai dati che arrivano attraverso il protocollo HTTP e inoltre previene l'esecuzione di script pericolosi sul computer.

La protezione Web controlla solo il traffico HTTP che passa attraverso le porte incluse nell'elenco di porte monitorate. Nel pacchetto Kaspersky Anti-Virus è incluso un elenco di porte comunemente utilizzate per il trasferimento della posta elettronica e del traffico HTTP. Se l'utente usa porte non comprese nell'elenco, dovrà aggiungerle per proteggere il traffico da esse gestito.

Se si lavora in un'area non protetta, è consigliabile utilizzare Anti-Virus Web durante la navigazione in Internet. Se il computer è inserito in una rete protetta da un firewall di filtri del traffico HTTP, Anti-Virus Web fornisce un'ulteriore protezione durante l'uso di Internet.

Una raccolta di impostazioni, denominata livello di protezione, determina la modalità di scansione del traffico. Se Anti-Virus Web rileva una minaccia, eseguirà l'azione assegnata.

Il livello di protezione del traffico Web è determinato da un insieme di impostazioni. Tali impostazioni possono essere suddivise nei gruppi seguenti:

- impostazioni dell'ambito di protezione;
- impostazioni che determinano l'efficienza della protezione del traffico (l'utilizzo dell'analisi euristica, ottimizzazione della scansione).

Kaspersky Lab consiglia di non configurare manualmente le impostazioni del componente Anti-Virus Web. Nella maggior parte dei casi è sufficiente selezionare un livello di protezione diverso.

➡ *Per modificare le impostazioni di Anti-Virus Web:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Apportare le modifiche richieste alle impostazioni dell'applicazione.

IN QUESTA SEZIONE:

Algoritmo di funzionamento del componente.....	61
Modifica del livello di protezione del traffico HTTP	62
Modifica delle azioni da eseguire sugli oggetti rilevati	62
Creazione di un ambito di protezione	63
Selezione del tipo di scansione	63
Barra degli strumenti degli URL di Kaspersky	64
Utilizzo dell'analisi euristica	65
Ottimizzazione della scansione	66
Ripristino delle impostazioni di protezione Web predefinite.....	66

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Anti-Virus Web protegge il computer verificando i dati che entrano nel computer tramite HTTP e impedisce l'esecuzione di script pericolosi nel computer.

In questa sezione viene descritto in modo più dettagliato il funzionamento del componente. Il traffico HTTP viene protetto mediante l'algoritmo seguente:

1. Ogni pagina Web o file a cui l'utente o un determinato programma può accedere attraverso il protocollo HTTP viene intercettato e analizzato da Anti-Virus Web per escludere la presenza di codice dannoso. Gli oggetti dannosi vengono rilevati utilizzando i database e l'algoritmo euristico di Kaspersky Anti-Virus. Il database contiene le descrizioni di tutti i programmi dannosi attualmente conosciuti, nonché i metodi che consentono di neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti nel database.
2. Dopo l'analisi è possibile agire come segue:
 - Se una pagina Web o un oggetto al quale l'utente cerca di accedere contengono codice dannoso, l'accesso a tale oggetto o pagina Web viene bloccato. Viene visualizzata una notifica relativa all'infezione dell'oggetto o della pagina richiesta.
 - Se il file o la pagina Web non contiene codice dannoso, il programma concede immediatamente l'accesso all'utente.

Gli script vengono esaminati secondo l'algoritmo seguente:

1. Ogni esecuzione di uno script su una pagina Web viene intercettata da Anti-Virus Web e analizzata per individuare eventuali codici dannosi.
2. Se lo script contiene codice dannoso, Anti-Virus Web lo blocca, informando l'utente con un apposito messaggio a comparsa.
3. Se nello script non viene rilevato alcun codice dannoso, esso viene eseguito.

Gli script vengono intercettati solo nelle pagine Web aperte in Microsoft Internet Explorer.

MODIFICA DEL LIVELLO DI PROTEZIONE DEL TRAFFICO HTTP

Il livello di protezione è definito come configurazione preimpostata delle impostazioni del componente Anti-Virus File. Gli specialisti di Kaspersky Lab distinguono tre livelli di protezione. Per decidere quale livello selezionare, l'utente deve considerare le condizioni operative e la situazione corrente. Come livello di protezione è possibile selezionare una delle opzioni elencate di seguito:

- **Alto.** Questo livello di protezione è consigliato in ambienti sensibili in cui non vengono utilizzati altri strumenti di protezione HTTP.
- **Consigliato.** Questo livello di protezione rappresenta la scelta ideale nella maggior parte delle situazioni.
- **Basso.** Utilizzare questo livello di protezione se nel computer sono installati altri strumenti di protezione del traffico HTTP.

Se nessuno dei livelli preimpostati soddisfa le proprie esigenze, è possibile configurare le impostazioni di Anti-Virus Web (vedere la sezione "Protezione del traffico Web" a pagina [60](#)). Di conseguenza, il nome del livello di protezione verrà modificato in **Personalizzato**. Per ripristinare le impostazioni predefinite del componente, selezionare uno dei livelli di protezione preimpostati.

➡ *Per modificare il livello di protezione preimpostato per il traffico Web:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Impostare il livello di protezione necessario per il componente selezionato.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Se l'analisi di un oggetto HTTP indica che questo contiene codice dannoso, la risposta del componente Anti-Virus Web dipende dall'azione selezionata dall'utente.

Anti-Virus Web blocca sempre le azioni eseguite da oggetti pericolosi e genera messaggi pop-up che comunicano all'utente l'azione intrapresa. L'azione su uno script pericoloso non può essere modificata. L'unica modifica possibile è la disabilitazione del modulo di scansione dello script (vedere la sezione "Selezione del tipo di scansione" a pagina [63](#)).

Se si lavora in modalità automatica (vedere la sezione "Passaggio 2. Selezione della modalità di protezione" a pagina [29](#)), Kaspersky Anti-Virus applicherà automaticamente l'azione consigliata dagli specialisti di Kaspersky Lab quando vengono rilevati oggetti pericolosi.

➡ *Per modificare l'azione specificata da eseguire sugli oggetti rilevati:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Specificare l'azione necessaria per il componente selezionato.

CREAZIONE DI UN AMBITO DI PROTEZIONE

La creazione di un ambito di protezione consiste nella selezione del tipo di scansione (vedere la sezione "Selezione del tipo di scansione" a pagina [63](#)) degli oggetti con Anti-Virus Web e nella creazione dell'elenco di indirizzi Web attendibili, che contiene informazioni non sottoposte a scansione da parte del componente per rilevare la presenza di oggetti pericolosi.

È possibile creare un elenco di indirizzi Web attendibili i cui contenuti sono ritenuti assolutamente innocui. Anti-Virus Web non analizzerà i dati provenienti da tali indirizzi per verificare la presenza di oggetti pericolosi. Questa opzione può risultare utile nei casi ad esempio in cui Anti-virus Web interferisce con il download di un file specifico.

➡ Per creare l'elenco di indirizzi Web attendibili, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra **Anti-Virus Web** visualizzata, sezione **Ottimizzazione della scansione**, selezionare la casella ☒ **Non esaminare il traffico HTTP per gli indirizzi attendibili** e cliccare sul bottone **Seleziona**.
5. Nella finestra **Elenco degli indirizzi Web bloccati** visualizzata, cliccare sul collegamento **Aggiungi**.
6. Immettere un indirizzo affidabile (o la relativa maschera) nella finestra **Maschera per l'indirizzo (URL)** visualizzata.

SELEZIONE DEL TIPO DI SCANSIONE

L'attività di creazione di un ambito di protezione (vedere pagina [63](#)), insieme alla creazione dell'elenco di indirizzi Web attendibili, include anche la selezione del tipo di scansione del traffico eseguita da Anti-Virus Web. A seconda del tipo, la scansione viene divisa tra scansione degli script e la scansione del traffico HTTP.

Per impostazione predefinita, Anti-Virus Web esegue la scansione del traffico HTTP e degli script simultaneamente.

La scansione del traffico HTTP include non solo la scansione anti-virus ma anche la verifica dei collegamenti per controllare che non siano inclusi nell'elenco di indirizzi Web sospetti e/o nell'elenco di indirizzi Web di phishing.

Il controllo dei collegamenti per verificare che non siano inclusi nell'elenco di indirizzi Web di phishing consente di evitare attacchi di phishing che, in genere, si presentano sotto forma di messaggi di posta elettronica provenienti da sedicenti istituti finanziari e contengono collegamenti ai relativi siti Web. Il testo del messaggio induce il lettore a cliccare sul collegamento e a immettere informazioni riservate nella finestra che segue, ad esempio, un numero di carta di credito o il nome utente e la password usati per collegarsi al proprio sito di Internet banking per eseguire operazioni finanziarie.

Poiché è possibile ricevere il collegamento a un sito di phishing non solo in un messaggio di posta elettronica ma attraverso altri veicoli, ad esempio nel testo di un messaggio ICQ, il componente Anti-Virus Web tiene traccia dei tentativi di accesso a un sito di phishing a livello di scansione del traffico HTTP e li blocca.

Il controllo dei collegamenti per verificare che non siano inclusi nell'elenco di indirizzi Web sospetti consente di tenere traccia dei siti Web inclusi nell'elenco Bloccati. L'elenco viene creato dagli specialisti di Kaspersky Lab ed è integrato nel pacchetto di installazione dell'applicazione.

➡ *Per consentire la scansione degli script da parte di Anti-Virus Web, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra **Anti-Virus Web** visualizzata, nel blocco **Avanzate**, verificare che la casella ☒ **Blocca gli script pericolosi in Microsoft Internet Explorer** sia selezionata. Anti-Virus Web eseguirà la scansione di tutti gli script elaborati in Microsoft Internet Explorer, nonché di qualsiasi altro script WSH (JavaScript, Visual Basic Script e così via) avviato durante l'utilizzo del computer da parte dell'utente.

È inoltre possibile utilizzare la barra degli strumenti degli URL di Kaspersky (vedere pagina [64](#)). A tale scopo, selezionare la casella ☒ **Segnala gli URL sospetti o di phishing in Microsoft Internet Explorer e Mozilla Firefox**. Anti-Virus Web contrassegnerà gli URL sospetti e di phishing di indirizzi Web rilevati nei browser (Microsoft Internet Explorer e Mozilla Firefox).

➡ *Per eseguire la scansione dei collegamenti utilizzando il database di indirizzi Web sospetti e/o di indirizzi Web di phishing, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra **Anti-Virus Web** visualizzata, sezione **Metodi di scansione**, verificare che le caselle ☒ **Confronta gli URL con il database degli indirizzi sospetti** e/o ☒ **Confronta gli URL con il database degli indirizzi di phishing** siano selezionate.

BARRA DEGLI STRUMENTI DEGLI URL DI KASPERSKY

Kaspersky Anti-Virus include il modulo di scansione degli URL gestito da Anti-Virus Web. Tale modulo verifica se i collegamenti presenti nella pagina Web appartengono all'elenco degli indirizzi Web di phishing o sospetti. È possibile creare un elenco di indirizzi Web attendibili il cui contenuto non deve essere sottoposto a scansione e un elenco di indirizzi Web il cui contenuto deve invece essere necessariamente sottoposto a scansione. Questo modulo è incorporato come plug-in nei browser Microsoft Internet Explorer e Mozilla Firefox.

➡ *Per abilitare la barra degli strumenti degli URL di Kaspersky, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Nella sezione **Livello di protezione** cliccare sul bottone **Impostazioni** per il componente selezionato.
4. Nella finestra **Anti-Virus Web** visualizzata, sezione **Avanzate**, selezionare la casella ☒ **Segnala gli URL sospetti o di phishing in Microsoft Internet Explorer e Mozilla Firefox**.

➡ Per creare l'elenco di indirizzi Web attendibili, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Nella sezione **Livello di protezione** cliccare sul bottone **Impostazioni** per il componente selezionato.
4. Nella finestra **Anti-Virus Web** visualizzata, sezione **Avanzate**, cliccare sul bottone **Impostazioni**.
5. Nella finestra **Barra degli strumenti di Kaspersky** visualizzata, selezionare l'opzione  **In tutte le pagine Web** e cliccare sul bottone **Esclusioni**.
6. Nella finestra **Elenco degli indirizzi Web bloccati** visualizzata, cliccare sul collegamento **Aggiungi**.
7. Immettere un indirizzo affidabile (o la relativa maschera) nella finestra **Maschera per l'indirizzo (URL)** visualizzata.

➡ Per creare l'elenco dei siti Web il cui contenuto deve essere sottoposto a scansione:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Nella sezione **Livello di protezione** cliccare sul bottone **Impostazioni** per il componente selezionato.
4. Nella finestra **Anti-Virus Web** visualizzata, sezione **Avanzate**, cliccare sul bottone **Impostazioni**.
5. Nella finestra **Barra degli strumenti di Kaspersky** visualizzata, selezionare l'opzione  **In tutte le pagine Web** e cliccare sul bottone **Esclusioni**.
6. Nella finestra **Elenco degli indirizzi Web bloccati** visualizzata, cliccare sul collegamento **Aggiungi**.
7. Nella finestra **Maschera per l'indirizzo (URL)** visualizzata, immettere l'indirizzo Web o la relativa maschera.

UTILIZZO DELL'ANALISI EURISTICA

Il metodo euristico implica l'analisi delle attività eseguite dall'oggetto nel sistema. Se tali azioni sono tipiche di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto. In questo modo è possibile rilevare le nuove minacce prima ancora che queste vengano studiate dagli analisti anti-virus. L'analisi euristica è abilitata per impostazione predefinita.

Kaspersky Anti-Virus informa l'utente della presenza di un oggetto nocivo rilevato in un messaggio. È necessario rispondere alla notifica elaborando ulteriormente il messaggio.

È inoltre possibile impostare il livello di dettaglio per le scansioni: **superficiale**, **media** o **approfondita**. spostando il cursore nella posizione selezionata.

➡ Per abilitare/disabilitare l'analisi euristica e impostare il livello di dettaglio della scansione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra **Anti-Virus Web** visualizzata, sezione **Metodi di scansione**, selezionare/deselezionare la casella  **Analisi euristica** e specificare il livello di dettaglio della scansione in basso per il componente selezionato.

OTTIMIZZAZIONE DELLA SCANSIONE

Per rilevare il codice nocivo in modo più efficiente, il componente Anti-Virus Web memorizza nel buffer frammenti di oggetti scaricati da Internet. Quando si utilizza questo metodo, un oggetto viene esaminato solo dopo essere stato scaricato completamente. Al termine del download viene sottoposto a scansione e, in base ai risultati ottenuti, viene restituito all'utente per poter essere utilizzato o bloccato.

La memorizzazione nel buffer comporta tuttavia un aumento dei tempi di elaborazione dell'oggetto e di conseguenza dei tempi di restituzione all'utente. Questo può causare problemi durante la copia e l'elaborazione di oggetti di grandi dimensioni in quanto è possibile che la connessione al client HTTP raggiunga il timeout.

Per risolvere questo problema, si consiglia di ridurre il tempo di memorizzazione nel buffer dei frammenti di oggetti Web scaricati da Internet. Allo scadere di questo limite temporale, l'utente riceve la parte scaricata e non esaminata del file. L'oggetto viene sottoposto a una scansione anti-virus solo dopo essere stato copiato completamente. Di conseguenza, il periodo di tempo necessario per trasferire l'oggetto all'utente si riduce, eliminando del tutto il problema della disconnessione. Inoltre, il livello di protezione per l'utilizzo di Internet non subisce variazioni.

Per impostazione predefinita, il tempo di memorizzazione nel buffer dei frammenti di file è limitato a un secondo. Aumentare questo valore o rimuovere il tempo limite di memorizzazione nel buffer migliora le scansioni anti-virus, ma rallenta l'accesso all'oggetto.

➡ *Per impostare un limite temporale per la memorizzazione nel buffer dei frammenti o per rimuoverlo, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra **Anti-Virus Web** visualizzata, sezione **Ottimizzazione della scansione**, selezionare/deselezionare la casella ☒ **Limita il tempo di creazione del buffer dei frammenti** e immettere il valore temporale (in secondi) nel campo a destra.

RIPRISTINO DELLE IMPOSTAZIONI DI PROTEZIONE WEB PREDEFINITE

Quando si configura Anti-Virus Web, è sempre possibile ripristinarne le impostazioni consigliate. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Esse sono raggruppate nel livello di protezione **Consigliato**.

➡ *Per ripristinare le impostazioni predefinite di Anti-Virus Web, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Nella sezione **Livello di protezione**, cliccare sul bottone **Livello predefinito** relativo al componente selezionato.

PROTEZIONE DEL TRAFFICO DEI PROGRAMMI DI MESSAGGISTICA ISTANTANEA

Oltre alle nuove funzionalità che rendono più semplice e agevole la navigazione in Internet, la grande diffusione dei client di messaggistica istantanea (d'ora in avanti definiti *client IM*), sta generando minacce potenziali alla protezione del computer. I messaggi che contengono URL di siti Web sospetti e quelli utilizzati da utenti malintenzionati per attacchi di phishing possono essere trasferiti tramite client IM. I programmi nocivi utilizzano infatti questo tipo di client per inviare messaggi di spamming e URL di programmi, o i programmi stessi, che rubano gli ID e le password degli utenti.

Il componente *Anti-Virus IM* è progettato per garantire il funzionamento dei client IM e per proteggere le informazioni che il computer riceve tramite protocolli IM.

Il prodotto protegge numerose applicazioni di messaggistica istantanea tra cui, ad esempio ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent e IRC.

Le applicazioni Yahoo! Messenger e Google Talk utilizzano il protocollo SSL. Per consentire ad Anti-Virus IM di eseguire la scansione del traffico di queste applicazioni, è necessario utilizzare la scansione delle connessioni crittografate (vedere pagina [111](#)). A tale scopo, selezionare la casella ☒ **Scansione delle connessioni crittografate** nella sezione **Rete**.

Il traffico viene analizzato in base a una determinata combinazione di impostazioni. Se in un messaggio vengono rilevate minacce, Anti-Virus IM sostituisce il messaggio con un messaggio di errore per l'utente.

Il livello di protezione del traffico IM è determinato da un insieme di impostazioni. Tali impostazioni possono essere suddivise nei gruppi seguenti:

- impostazioni per la creazione dell'ambito di protezione;
- impostazioni per la determinazione dei metodi di scansione.

➡ Per modificare le impostazioni di Anti-Virus IM, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus IM**.
3. Apportare le modifiche desiderate alle impostazioni del componente selezionato.

IN QUESTA SEZIONE:

Algoritmo di funzionamento del componente.....	67
Creazione di un ambito di protezione	68
Selezione del metodo di scansione	68
Utilizzo dell'analisi euristica	69

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

In Kaspersky Anti-Virus è incluso un componente, denominato *Anti-Virus IM*, che garantisce la scansione dei messaggi trasferiti tramite client di messaggistica istantanea per l'individuazione di oggetti pericolosi. Tale componente viene caricato all'avvio del sistema operativo ed eseguito nella RAM del computer. Esamina tutti i messaggi in entrata e in uscita.

Per impostazione predefinita, la protezione del traffico dei client di messaggistica istantanea viene garantita mediante l'algoritmo descritto di seguito:

1. Ogni messaggio ricevuto o inviato dall'utente viene intercettato dal componente.
2. Anti-Virus IM esegue la scansione del messaggio per rilevare eventuali oggetti pericolosi o URL elencati nei database degli indirizzi Web sospetti e/o di phishing. Se viene individuata una minaccia, il testo del messaggio viene sostituito con un messaggio di avviso per l'utente.
3. Se non vengono individuate minacce per la protezione, il messaggio viene reso disponibile per l'utente.

I file trasferiti tramite client IM vengono esaminati dal componente Anti-Virus File (vedere la sezione "Protezione del file system del computer" a pagina [43](#)) quando si tenta di eseguirne il salvataggio.

CREAZIONE DI UN AMBITO DI PROTEZIONE

Per ambito di protezione si intende il tipo di messaggi da esaminare.

-  **Messaggi in entrata e in uscita.** Anti-Virus IM esamina i messaggi sia in entrata che in uscita per impostazione predefinita.
-  **Solo messaggi in entrata.** Se si è certi che i messaggi inviati non contengano oggetti pericolosi, selezionare questa impostazione. Anti-Virus IM esaminerà solo i messaggi in entrata.

Per impostazione predefinita, Kaspersky Anti-Virus esamina sia i messaggi in entrata che in uscita dei client IM.

Se si è certi che i messaggi inviati non contengano oggetti pericolosi, è possibile disabilitare la scansione del traffico in uscita.

➔ Per disabilitare la scansione dei messaggi in uscita, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus IM**.
3. Nella sezione **Ambito della protezione**, selezionare l'opzione  **Solo messaggi in entrata** relativa al componente selezionato.

SELEZIONE DEL METODO DI SCANSIONE

I metodi di scansione consistono nella scansione degli URL nei messaggi inviati dai client di messaggistica istantanea per verificare che non siano inclusi nell'elenco di indirizzi Web sospetti e/o nell'elenco di indirizzi Web di phishing.

-  **Confronta gli URL con il database degli indirizzi sospetti.** Anti-Virus IM esegue una scansione dei collegamenti all'interno dei messaggi per verificare se sono inclusi nella lista nera.
-  **Confronta gli URL con il database degli indirizzi di phishing.** I database di Kaspersky Anti-Virus includono tutti i siti attualmente noti utilizzati per gli attacchi di phishing. Kaspersky Lab arricchisce questo elenco con gli indirizzi ottenuti da Anti-Phishing Working Group, un'organizzazione internazionale. L'elenco viene aggiornato durante l'aggiornamento dei database di Kaspersky Anti-Virus.

➡ *Per eseguire la scansione dei collegamenti nei messaggi utilizzando il database di indirizzi Web sospetti, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus IM**.
3. Nella sezione **Metodi di scansione**, selezionare la casella ☒ **Confronta gli URL con il database degli indirizzi sospetti** relativa al componente selezionato.

➡ *Per eseguire la scansione dei collegamenti nei messaggi utilizzando il database di indirizzi Web di phishing, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus IM**.
3. Nella sezione **Metodi di scansione**, selezionare la casella ☒ **Confronta gli URL con il database degli indirizzi di phishing** relativa al componente selezionato.

UTILIZZO DELL'ANALISI EURISTICA

Il metodo euristico implica l'analisi delle attività eseguite dall'oggetto nel sistema. A tale scopo, qualsiasi script incluso nel messaggio di un client IM viene eseguito nell'ambiente protetto. Se l'attività dello script è tipica di oggetti nocivi, è probabile che l'oggetto venga classificato come nocivo o sospetto. L'analisi euristica è abilitata per impostazione predefinita.

Kaspersky Anti-Virus informa l'utente della presenza di un oggetto nocivo rilevato in un messaggio.

È inoltre possibile impostare il livello di dettaglio per le scansioni: **Superficiale**, **Media** o **Approfondita**, spostando il cursore nella posizione selezionata.

➡ *Per abilitare/disabilitare l'analisi euristica e impostare il livello di dettaglio della scansione, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus IM**.
3. Nella sezione **Metodi di scansione**, selezionare/deselezionare la casella ☒ **Analisi euristica** e impostare il livello di dettaglio della scansione in basso per il componente selezionato.

DIFESA PROATTIVA

Kaspersky Anti-Virus protegge sia da minacce note che da quelle nuove, sulle quali i database dell'applicazione non includono alcuna informazione. Questa funzione è garantita da un componente specifico denominato *Difesa Proattiva*.

Le tecnologie preventive offerte da Difesa Proattiva neutralizzano le nuove minacce prima che possano danneggiare il computer. A differenza delle tecnologie reattive, che analizzano il codice in base ai record contenuti nei database di Kaspersky Anti-Virus, le tecnologie preventive riconoscono una nuova minaccia sul computer tramite una sequenza di azioni eseguite da un programma. Se, come risultato dell'analisi delle attività, la sequenza di azioni dell'applicazione desta sospetti, Kaspersky Anti-Virus blocca l'attività dell'applicazione.

► Per modificare le impostazioni di Difesa Proattiva, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
3. Apportare le modifiche desiderate alle impostazioni per il componente selezionato.

IN QUESTA SEZIONE:

Utilizzo dell'elenco di attività pericolose.....	70
Modifica delle regole per il monitoraggio delle attività pericolose	71
Creazione di un gruppo di applicazioni attendibili.....	72
Controllo degli account di sistema	72

UTILIZZO DELL'ELENCO DI ATTIVITÀ PERICOLOSE

Tenere presente che la configurazione delle impostazioni per il controllo delle attività di Kaspersky Anti-Virus in Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7, Microsoft Windows 7 x64, Microsoft Windows 7 o Microsoft Windows 7 x64 presenta alcune differenze rispetto ad altri sistemi operativi.

Specifiche per la configurazione del controllo delle attività delle applicazioni in Microsoft Windows XP

Kaspersky Anti-Virus controlla l'attività dell'applicazione sul computer. Difesa Proattiva reagisce immediatamente a una sequenza definita di azioni delle applicazioni. Quando, ad esempio, viene individuato un programma che esegue azioni come copiare se stesso nelle risorse di rete, nella cartella di avvio o nel Registro di sistema per poi inviare copie di se stesso, è molto probabile che si tratti di un worm. Altre sequenze di operazioni pericolose includono:

- azioni tipiche di programmi Trojan;
- tentativi di intercettazione della tastiera;
- installazione nascosta di driver;
- tentativi di modifica del kernel del sistema operativo;
- tentativi di creazione di oggetti e processi nascosti con PID negativo;
- tentativi di modifica dei file HOSTS;
- tentativi di implementazione in altri processi;
- rootkit che reindirizzano l'input/output dei dati;
- tentativi di invio di richieste DNS.

L'elenco di attività pericolose viene aggiunto automaticamente in seguito all'aggiornamento di Kaspersky Anti-Virus e non è modificabile. È tuttavia possibile disattivare il monitoraggio di un'attività pericolosa.

➡ *Per disattivare il monitoraggio di un'attività pericolosa:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra **Difesa Proattiva** visualizzata, deselezionare la casella ☒ accanto al nome dell'attività che non si desidera monitorare.

Specifiche per la configurazione del controllo delle attività delle applicazioni in Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 o Microsoft Windows 7 x64

Se il computer è in esecuzione in uno dei sistemi operativi indicati sopra, il controllo non verrà applicato a ogni evento a causa delle caratteristiche specifiche di tali sistemi. Il controllo, ad esempio, non verrà applicato ai tipi di eventi seguenti: *intrusione in un altro processo, invio di dati mediante applicazioni attendibili, attività di sistema sospette, accesso a memoria protetta.*

MODIFICA DELLE REGOLE PER IL MONITORAGGIO DELLE ATTIVITÀ PERICOLOSE

L'elenco di attività pericolose viene aggiunto automaticamente in seguito all'aggiornamento di Kaspersky Anti-Virus e non è modificabile. È possibile:

- disattivare il monitoraggio di un'attività pericolosa;
- modificare la regola utilizzata da Difesa Proattiva quando viene rilevata un'attività pericolosa;
- creare un elenco di esclusioni (vedere pagina [108](#)), elencando le applicazioni la cui attività non viene considerata pericolosa.

➡ *Per modificare la regola:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
3. Cliccare sul bottone **Impostazioni** relativo al componente selezionato.
4. Nella finestra **Difesa Proattiva** visualizzata, sezione **Eventi**, selezionare l'evento per il quale si desidera modificare la regola.
5. Configurare le impostazioni dell'evento selezionato utilizzando i collegamenti nella sezione di descrizione delle regole:
 - cliccare sul collegamento con l'azione preimpostata e selezionare l'azione desiderata nella finestra **Seleziona azione** visualizzata.
 - cliccare sul collegamento con il periodo di tempo preimpostato (non per tutti i tipi di attività) e specificare l'intervallo di scansione per i processi nascosti nella finestra **Rilevamento di processi nascosti** visualizzata.
 - cliccare sul collegamento **Attivato/Disattivato** per indicare che è necessario creare il rapporto sull'esecuzione dell'attività.

CREAZIONE DI UN GRUPPO DI APPLICAZIONI ATTENDIBILI

È possibile utilizzare l'opzione che consente di specificare l'intervallo di applicazioni attendibili, le cui attività non verranno esaminate da Difesa Proattiva. Le applicazioni attendibili possono essere applicazioni con una firma digitale o incluse nel database di Kaspersky Security Network.

- *Se si desidera che Difesa Proattiva consideri le applicazioni con una firma digitale e/o contenute nel database di Kaspersky Security Network come attendibili e non ne notifichi l'attività, eseguire le operazioni seguenti:*
1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
 2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
 3. Nella sezione **Applicazioni attendibili**, selezionare la casella ☒ **Applicazioni con firma digitale** e/o la casella ☒ **Applicazioni del database di Kaspersky Security Network** per il componente selezionato.

CONTROLLO DEGLI ACCOUNT DI SISTEMA

Gli account utente controllano l'accesso al sistema e identificano l'utente e il relativo ambiente di lavoro, impedendo ad altri utenti di danneggiare il sistema operativo e i dati. I processi di sistema sono processi avviati dagli account utente di sistema.

- *Se si desidera controllare l'attività dei processi di sistema oltre a quella dei processi utente mediante Kaspersky Anti-Virus, eseguire le operazioni seguenti:*
1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
 2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
 3. Nella sezione **Avanzate**, selezionare la casella ☒ **Effettua il monitoraggio degli account utente del sistema** relativa al componente selezionato.

SCANSIONE DEL COMPUTER

La scansione del computer per cercare eventuali virus e vulnerabilità è una delle attività più importanti per garantire la sicurezza del computer. La scansione anti-virus consente di rilevare la diffusione di codice dannoso che per qualche motivo non è stato rilevato dalla protezione malware. La ricerca delle vulnerabilità consente di rilevare le vulnerabilità software che gli utenti malintenzionati possono utilizzare per diffondere oggetti dannosi e ottenere l'accesso a informazioni personali.

Kaspersky Lab distingue tra le varie attività di scansione anti-virus (vedere pagina [73](#)), inclusa la scansione delle unità rimovibili (vedere pagina [79](#)) e la scansione della vulnerabilità del sistema e delle applicazioni (vedere pagina [84](#)).

► Per modificare le impostazioni di qualsiasi attività di scansione:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**, **Scansione Vulnerabilità**).
3. Apportare le modifiche desiderate alle impostazioni dell'attività selezionata.

IN QUESTA SEZIONE:

Scansione anti-virus	73
Scansione Vulnerabilità	84

SCANSIONE ANTI-VIRUS

Gli specialisti di Kaspersky Lab distinguono diversi tipi di attività di scansione anti-virus:

- **Scansione Oggetti.** Gli oggetti selezionati dall'utente vengono sottoposti a scansione. È possibile eseguire la scansione di tutti gli oggetti del file system del computer. Durante questa attività è possibile configurare le impostazioni per la scansione delle unità rimovibili.
- **Scansione Completa.** Una scansione approfondita dell'intero sistema. Per impostazioni predefinita, vengono sottoposti a scansione gli oggetti seguenti: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di messaggi e-mail, dischi fissi, supporti di archiviazione rimovibili e unità di rete.
- **Scansione Rapida.** Viene eseguita la scansione degli oggetti di avvio del sistema operativo.

Le attività Scansione Completa e Scansione Rapida sono attività specifiche. È consigliabile non modificare l'elenco di oggetti esaminati da queste attività.

Ogni attività di scansione viene eseguita nell'area specificata e può essere avviata in base alla pianificazione creata. Un insieme di parametri delle attività di scansione anti-virus definisce il livello di protezione. Per impostazione predefinita, sono disponibili tre livelli.

In seguito all'avvio della scansione anti-virus, il relativo stato di avanzamento viene visualizzato nella sezione **Scansione** della finestra principale dell'applicazione, nel campo con il nome dell'attività avviata. Se viene rilevata una minaccia, l'applicazione esegue l'azione specificata.

Durante la ricerca di minacce, le informazioni sui risultati vengono registrate in un rapporto di Kaspersky Anti-Virus.

È inoltre possibile selezionare un oggetto da esaminare con gli strumenti standard del sistema operativo Microsoft Windows, ad esempio nella finestra del programma **Esplora risorse** o sul **Desktop**. Posizionare il cursore sul nome dell'oggetto desiderato, cliccare con il pulsante destro del mouse per aprire il menu di scelta rapida di Microsoft Windows e scegliere l'opzione **Scansione Anti-Virus del file**.



Figura 9. Menu di scelta rapida di Microsoft Windows

È inoltre possibile visualizzare il rapporto di scansione contenente tutte le informazioni relative agli eventi verificatisi durante l'esecuzione dell'attività.

VEDERE ANCHE:

Avvio dell'attività di scansione anti-virus.....	75
Creazione di un collegamento per l'esecuzione di attività	76
Creazione di un elenco di oggetti da esaminare.....	76
Modifica del livello di protezione	77
Modifica delle azioni da eseguire sugli oggetti rilevati	77
Modifica del tipo di oggetti da esaminare	78
Ottimizzazione della scansione	79
Scansione di unità disco rimovibili.....	79
Scansione di file compositi	80
Tecnologia di scansione	81
Modifica del metodo di scansione	81
Modalità di esecuzione: creazione di una pianificazione	82
Modalità di esecuzione: specifica di un account.....	83
Funzionalità dell'avvio pianificato delle attività.....	83
Ripristino delle impostazioni di scansione predefinite.....	83

AVVIO DELL'ATTIVITÀ DI SCANSIONE ANTI-VIRUS

Un'attività di scansione anti-virus può essere avviata in uno dei modi seguenti:

- dal menu di scelta rapida di Kaspersky Anti-Virus (vedere la sezione "Menu di scelta rapida" a pagina [39](#));
- dalla finestra principale dell'applicazione (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [40](#));
- utilizzando un collegamento esistente (vedere pagina [76](#)).

Le informazioni sull'esecuzione dell'attività verranno visualizzate nella finestra principale di Kaspersky Anti-Virus.

È inoltre possibile selezionare l'oggetto da esaminare utilizzando gli strumenti standard del sistema operativo Microsoft Windows, ad esempio dalla finestra di **Esplora** risorse, dal **Desktop** e così via.



Figura 10. menu di scelta rapida di Microsoft Windows

► Per avviare l'attività utilizzando un collegamento:

1. Aprire la cartella in cui è stato creato un collegamento.
2. Avviare l'attività facendo doppio clic su un collegamento. Lo stato di avanzamento dell'esecuzione dell'attività verrà visualizzato nella finestra principale di Kaspersky Anti-Virus nella sezione **Scansione**.

► Per avviare un'attività anti-virus dal menu di scelta rapida dell'applicazione:

1. Cliccare con il pulsante destro del mouse sull'icona nell'area di notifica della barra delle applicazioni.
2. Selezionare la voce **Scansione Anti-Virus** nel menu di scelta rapida visualizzato.
3. Nella finestra principale di Kaspersky Anti-Virus visualizzata, nella sezione **Scansione**, cliccare sul bottone con il nome dell'attività richiesta.

Per avviare la scansione completa del computer, selezionare la voce **Scansione Completa** dal menu di scelta rapida. Verrà avviata una scansione completa del computer. Lo stato di avanzamento dell'esecuzione dell'attività verrà visualizzato nella finestra principale di Kaspersky Anti-Virus nella sezione **Scansione**.

► Per avviare l'attività di scansione anti-virus dalla finestra principale dell'applicazione:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Cliccare sul bottone che riporta il nome dell'attività richiesta.

➤ Per avviare una scansione anti-virus di un oggetto selezionato dal menu di scelta rapida di Windows:

1. Cliccare con il pulsante destro del mouse sul nome dell'oggetto selezionato.
2. Selezionare la voce **Scansione Anti-Virus del file** nel menu di scelta rapida visualizzato. Lo stato di avanzamento e i risultati dell'esecuzione dell'attività verranno visualizzati nella finestra che si apre.

CREAZIONE DI UN COLLEGAMENTO PER L'ESECUZIONE DI ATTIVITÀ

L'applicazione offre l'opportunità di creare collegamenti per avviare rapidamente attività di scansione completa e attività di scansione rapida. Ciò consente di avviare l'attività di scansione richiesta senza aprire la finestra dell'applicazione principale o il menu di scelta rapida.

➤ Per creare un collegamento per l'avvio di un'attività di scansione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Nella parte destra della finestra, nel blocco **Esecuzione rapida delle attività** di scansione, cliccare sul bottone **Crea collegamento** accanto al nome dell'attività richiesta (**Scansione Rapida** oppure **Scansione Completa**).
4. Nella finestra che viene visualizzata specificare il percorso in cui salvare il collegamento. Per impostazione predefinita, il collegamento viene creato con il nome di un'attività nella cartella *Risorse del computer* dell'utente corrente.

CREAZIONE DI UN ELENCO DI OGGETTI DA ESAMINARE

Ogni scansione anti-virus comprende il relativo elenco predefinito di oggetti. Tali oggetti possono includere elementi del file system del computer, quali le unità logiche e i **database di posta** o altri tipi di oggetto quali le unità di rete. ma può essere modificato.

Gli oggetti vengono visualizzati nell'elenco subito dopo essere stati aggiunti. Se si seleziona la casella ☒ **Includi sottocartelle** mentre si aggiunge un oggetto, la scansione verrà eseguita in modo ricorsivo.

Per eliminare un oggetto dall'elenco, selezionarlo e cliccare sul collegamento **Elimina**.

Gli oggetti che appaiono nell'elenco per impostazione predefinita non possono essere modificati né eliminati.

Oltre a eliminare gli oggetti dall'elenco, è possibile anche ignorarli temporaneamente durante l'esecuzione di una scansione. A tal fine, selezionare l'oggetto dall'elenco e deselezionare la casella a sinistra del nome dell'oggetto.

Se l'ambito di scansione è vuoto o non contiene oggetti selezionati, l'attività di scansione non può essere avviata.

➤ Per creare l'elenco di oggetti per un'attività di scansione oggetti, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Cliccare sul collegamento **Aggiungi**.
4. Nella finestra **Scelta degli oggetti da esaminare** visualizzata selezionare un oggetto e cliccare sul bottone **Aggiungi**. Cliccare sul bottone **OK** dopo aver aggiunto tutti gli oggetti necessari. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella.

➡ Per creare l'elenco di oggetti da sottoporre a scansione rapida o completa, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra selezionare l'attività **Scansione Completa (Scansione Rapida)**.
3. Nel blocco **Ambito della scansione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra **<Nome attività di scansione>: elenco degli oggetti** visualizzata, creare l'elenco utilizzando i collegamenti **Aggiungi**, **Modifica**, **Elimina**. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella.

MODIFICA DEL LIVELLO DI PROTEZIONE

Il livello di protezione è una raccolta preimpostata delle impostazioni della scansione. Gli specialisti di Kaspersky Lab distinguono tre livelli di protezione. La decisione sul livello da selezionare si basa sulle preferenze personali. È possibile selezionare uno dei livelli di protezione seguenti:

- **Alto**. Questo livello deve essere impostato se si sospetta che la possibilità che il computer venga infettato sia alta.
- **Consigliato**. Si tratta del livello più appropriato nella maggior parte dei casi e in genere consigliato dagli specialisti Kaspersky Lab.
- **Basso**. Se si utilizzano applicazioni che richiedono quantità notevoli di risorse RAM, selezionare il livello di protezione basso in quanto in questa modalità l'applicazione impiega una quantità inferiore di risorse di sistema.

Se nessuno dei livelli preimpostati risulta soddisfacente, è possibile configurare la scansione manualmente. Di conseguenza, il nome del livello di protezione verrà modificato in **Personalizzato**. Per ripristinare le impostazioni predefinite di scansione, selezionare uno dei livelli di protezione preimpostati.

➡ Per modificare il livello di protezione definito, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nella sezione **Livello di protezione**, impostare il livello di protezione necessario per l'attività selezionata.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Alle minacce appena rilevate Kaspersky Anti-Virus assegna uno degli stati seguenti:

- programma dannoso, ad esempio nel caso di un *virus* o di un *Trojan*.
- *Potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Il dubbio sorge quando l'applicazione rileva nel file una sequenza di codice di un virus sconosciuto o il codice modificato di un virus conosciuto.

Se Kaspersky Anti-Virus rileva oggetti infetti o potenzialmente infetti durante una scansione anti-virus, ne dà notizia all'utente. È necessario rispondere alla minaccia imminente selezionando un'azione da eseguire sull'oggetto. Kaspersky Anti-Virus seleziona l'opzione **Chiedi di scegliere un'azione** come azione da eseguire su un oggetto rilevato, che rappresenta l'impostazione predefinita. È possibile modificare l'azione. Se, ad esempio, si desidera eseguire un tentativo di disinfezione per ogni oggetto rilevato ma non si desidera selezionare l'azione **Disinfetta** ogni volta che si riceve un avviso sul rilevamento di un oggetto infetto o sospetto, è necessario selezionare l'azione **Scegli l'azione automaticamente. Disinfetta**.

Prima di provare a disinfettare o eliminare un oggetto infetto, Kaspersky Anti-Virus ne crea una copia di backup per consentirne il ripristino o la disinfezione in un secondo momento.

Se si lavora in modalità automatica (vedere la sezione "Passaggio 2. Selezione della modalità di protezione" a pagina 29), Kaspersky Anti-Virus applicherà automaticamente l'azione consigliata dagli specialisti di Kaspersky Lab quando vengono rilevati oggetti pericolosi. Per gli oggetti dannosi, tale azione sarà **Disinfetta. Elimina se la disinfezione fallisce e Ignora** per gli oggetti sospetti.

➡ Per modificare l'azione specificata da eseguire sugli oggetti rilevati:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Azione** specificare l'azione richiesta per l'attività selezionata.

MODIFICA DEL TIPO DI OGGETTI DA ESAMINARE

Quando si specifica il tipo di oggetti da esaminare, vengono definiti il formato e le dimensioni dei file su cui verrà eseguita l'attività di scansione selezionata.

Quando si seleziona il tipo di file, è necessario tenere presente quanto segue:

- La probabilità di penetrazione di codice dannoso in diversi formati di file (ad esempio *txt*) e la successiva attivazione è molto bassa. Altri formati, al contrario, contengono o possono contenere codice eseguibile (*exe*, *dll*, *doc*). Il rischio di penetrazione ed attivazione di codice nocivo in tali file è piuttosto alto.
- È importante ricordare che un utente malintenzionato può inviare un virus al computer in un file con estensione *txt* che in realtà è un file eseguibile rinominato come *txt*. Selezionando l'opzione  **Esamina i file per estensione**, tale file viene ignorato dalla scansione. Se è stata selezionata l'opzione  **Esamina i file per formato**, la protezione del file analizza l'intestazione del file per determinare se si tratta di un file *exe*. Tale file sarà sottoposto ad una scansione anti-virus approfondita.

➡ Per modificare il tipo di oggetto esaminato:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Livello di protezione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, scheda **Ambito**, blocco **Tipi di file**, selezionare le impostazioni richieste.

OTTIMIZZAZIONE DELLA SCANSIONE

È possibile ridurre la durata della scansione e accelerare l'esecuzione dell'applicazione. Per ottenere questo risultato, è necessario eseguire la scansione solo dei file nuovi e dei file stati modificati dopo l'ultima scansione. Questa modalità si applica sia ai file semplici che composti.

È inoltre possibile ridurre il tempo di scansione per ciascun file specifico. Una volta trascorso l'intervallo di tempo specificato, la scansione del file viene interrotta.

➡ *Per eseguire la scansione solo dei file nuovi e dei file modificati:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Livello di protezione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Ambito**, sezione **Ottimizzazione della scansione**, selezionare la casella ☒ **Esamina solo i file nuovi e modificati**.

➡ *Per imporre una restrizione temporale alla durata della scansione:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Livello di protezione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Ambito**, sezione **Ottimizzazione della scansione**, selezionare la casella ☒ **Ignora i file analizzati per più di** e specificare la durata della scansione nel campo adiacente.

SCANSIONE DI UNITÀ DISCO RIMOVIBILI

Gli oggetti dannosi che utilizzano le vulnerabilità del sistema operativo per replicarsi tramite reti e supporti rimovibili si stanno diffondendo sempre di più.

Utilizzare l'opzione che consente di eseguire la scansione delle unità rimovibili nel momento in cui vengono collegate al computer. A tale scopo, è necessario selezionare una delle azioni da eseguire con Kaspersky Anti-Virus:

- **Non eseguire scansione.** Le unità disco rimovibili vengono esaminate automaticamente durante la connessione a un computer.
- **Chiedi all'utente.** Per impostazione predefinita, Kaspersky Anti-Virus richiede all'utente di eseguire azioni aggiuntive quando viene connessa un'unità rimovibile.
- **Scansione Completa.** Durante il collegamento di unità rimovibili, l'applicazione esegue una scansione completa dei file memorizzati al suo interno, in base alle impostazioni dell'attività Scansione Completa.
- **Scansione Rapida.** Durante il collegamento di unità rimovibili, tutti i file vengono esaminati in base alle impostazioni dell'attività Scansione Rapida.

➡ *Per utilizzare la funzionalità di scansione dei supporti rimovibili al momento della connessione, eseguire la procedura seguente:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Nella sezione **Scansione automatica delle unità rimovibili**, selezionare l'azione e, se necessario, definire la dimensione massima dell'unità da esaminare nel campo sottostante.

SCANSIONE DI FILE COMPOSITI

Un metodo comune per nascondere i virus consiste nell'incorporarli in file compositi, ovvero archivi, database e così via. Per individuare i virus nascosti in questo modo, è necessario decomprimere un file composito, operazione che può ridurre in modo significativo la velocità di scansione.

Per ogni tipo di file composito, è possibile scegliere di analizzare tutti i file oppure solo quelli nuovi. Per farlo, utilizzare il collegamento accanto al nome dell'oggetto. Il relativo valore verrà modificato quando si clicca con il bottone sinistro del mouse su di esso. Se si seleziona la modalità di scansione dei soli file nuovi e modificati (vedere pagina [79](#)), non sarà possibile selezionare i tipi di file compositi da sottoporre a scansione.

È possibile limitare la dimensione massima dei file compositi da esaminare. I file compositi di dimensioni maggiori di quelle specificate non saranno esaminati.

I file più grandi estratti dagli archivi verranno esaminati anche se la casella ☒ **Non decomprimere i file compositi di grandi dimensioni** è selezionata.

➡ *Per modificare l'elenco dei file compositi esaminati:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Livello di protezione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Ambito**, sezione **Scansione dei file compositi**, selezionare il tipo appropriato di file compositi da esaminare.

➡ *Per impostare la dimensione massima dei file compositi da esaminare:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Livello di protezione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Ambito**, sezione **Scansione dei file compositi**, scegliere il bottone **Avanzate**.
5. Nella finestra **File compositi** visualizzata, selezionare la casella ☒ **Non decomprimere i file compositi di grandi dimensioni** e specificare la dimensione di file nel campo adiacente.

TECNOLOGIA DI SCANSIONE

È possibile anche specificare la tecnologia che verrà utilizzata durante la scansione, scegliendo una delle due alternative disponibili:

- **iChecker.** Questa tecnologia è in grado di aumentare la velocità di scansione escludendo determinati oggetti dalla scansione. Un oggetto viene escluso dalla scansione utilizzando uno speciale algoritmo che prende in considerazione la data di rilascio del database del programma, la data dell'ultima scansione dell'oggetto e le modifiche alle impostazioni di scansione.

Si supponga, ad esempio, di disporre di un file archivio a cui dopo la scansione da parte di Kaspersky Anti-Virus è stato assegnato lo stato *non infetto*. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se la struttura dell'archivio risulta modificata perché è stato aggiunto un nuovo oggetto oppure se le impostazioni di scansione sono state modificate o i database dell'applicazione aggiornati, il programma esaminerà nuovamente l'archivio.

iChecker presenta tuttavia delle limitazioni: non funziona con file di grandi dimensioni ed è applicabile solo agli oggetti con una struttura riconosciuta dall'applicazione, ad esempio file .exe, .dll, .lnk, .tff, .inf, .sys, .com, .chm, .zip, .rar.

- **iSwift.** Questa tecnologia è stata sviluppata a partire dalla tecnologia iChecker per i computer che utilizzano un file system di tipo NTFS. Anche la tecnologia iSwift presenta delle limitazioni: è associata a un percorso di file specifico nel file system e può essere applicata solo a oggetti in NTFS.

➡ *Per cambiare tecnologia di scansione degli oggetti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Livello di protezione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Avanzate** della sezione **Tecnologie di scansione**, selezionare il valore di impostazione appropriato.

MODIFICA DEL METODO DI SCANSIONE

È possibile modificare le impostazioni di scansione che ne determinano l'accuratezza. Per impostazione predefinita, la modalità che utilizza le voci del database dell'applicazione per cercare le minacce è sempre abilitata. Inoltre, è possibile applicare diversi metodi e tecnologie di scansione (vedere pagina [81](#)).

La modalità di scansione, nella quale Kaspersky Anti-Virus confronta l'oggetto rilevato con i record dei database, è definita *analisi delle firme* e viene sempre applicata alla scansione. Inoltre, è sempre possibile utilizzare l'*analisi euristica*. Questo metodo presuppone l'analisi delle azioni eseguite da un oggetto all'interno del sistema. Se tali azioni sono tipiche di oggetti nocivi, è probabile che l'oggetto venga classificato come nocivo o sospetto.

Inoltre, è possibile selezionare il livello di dettaglio dell'analisi euristica: rapida, media o completa. spostando il cursore nella posizione selezionata.

Oltre a tali metodi di scansione è possibile utilizzare la scansione rootkit. I rootkit sono insiemi di strumenti in grado di nascondere i programmi dannosi nel sistema operativo. Queste utilità vengono inserite nel sistema, nascondendo la loro presenza e quella dei processi, delle cartelle e delle chiavi di registro di altri programmi dannosi installati con il rootkit. Se la scansione è abilitata, è possibile specificare il livello dettagliato (analisi avanzata) per la rilevazione dei rootkit che eseguono una scansione accurata di tali programmi attraverso l'analisi di un gran numero di oggetti di vario tipo.

➡ *Per specificare il metodo di scansione da utilizzare:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Modalità di esecuzione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Avanzate** della sezione **Metodi di scansione**, selezionare i valori richiesti per le impostazioni.

MODALITÀ DI ESECUZIONE: CREAZIONE DI UNA PIANIFICAZIONE

È possibile creare una pianificazione per avviare automaticamente le attività di scansione anti-virus.

L'impostazione principale riguarda l'intervallo di tempo tra gli avvii dell'attività. Per modificarla, specificare le impostazioni della pianificazione per l'opzione selezionata.

Se per qualsiasi motivo non è possibile avviare l'attività, ad esempio perché all'ora prevista il computer era spento, è possibile configurare l'attività in modo che venga avviata automaticamente non appena possibile.

➡ *Per modificare una pianificazione per le attività di scansione:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Modalità di esecuzione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Pianifica**, selezionare l'opzione **Manualmente** per avviare un'attività di scansione quando lo si ritiene più opportuno. Per eseguire l'attività periodicamente, selezionare **Pianifica** e creare una pianificazione di avvio dell'attività.

➡ *Per configurare l'avvio automatico delle attività ignorate:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Modalità di esecuzione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Pianifica**, selezionare la casella ☒ **Esegui le attività rimandate**.

MODALITÀ DI ESECUZIONE: SPECIFICA DI UN ACCOUNT

È possibile specificare un account utilizzato dall'applicazione durante l'esecuzione di una scansione anti-virus.

➡ *Per specificare un account:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Modalità di esecuzione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Account utente**, selezionare la casella ☒ **Esegui l'attività come**. Specificare il nome utente e la password.

FUNZIONALITÀ DELL'AVVIO PIANIFICATO DELLE ATTIVITÀ

Tutte le attività di scansione possono essere avviate manualmente o in base a una pianificazione.

Le attività pianificate includono funzionalità aggiuntive, ad esempio la possibilità di *sospendere la scansione pianificata quando lo screensaver è inattivo o il computer è sbloccato*. Questa funzionalità consente di rimandare l'avvio dell'attività finché l'utente non avrà terminato di lavorare al computer. Pertanto, l'attività di scansione non richiederà l'utilizzo delle risorse del sistema durante le ore lavorative.

➡ *Per avviare le attività di scansione solo quando il computer non è più in uso, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Modalità di esecuzione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Pianificazione**, selezionare la casella ☒ **Sospendi la scansione se lo screensaver non è attivo e il computer non è bloccato**.

RIPRISTINO DELLE IMPOSTAZIONI DI SCANSIONE PREDEFINITE

Quando si configurano le impostazioni delle attività, è sempre possibile ripristinare quelle consigliate. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Esse sono raggruppate nel livello di protezione **Consigliato**.

➡ *Per ripristinare le impostazioni di scansione dei file predefinite:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata)**.
3. Nel blocco **Livello di protezione**, cliccare sul bottone **Livello predefinito** per l'attività selezionata.

SCANSIONE VULNERABILITÀ

L'attività di ricerca delle vulnerabilità consiste nella diagnostica della protezione del sistema e nella ricerca di vulnerabilità potenziali utilizzate da utenti malintenzionati per arrecare danni ai computer.

Durante la ricerca delle vulnerabilità, l'applicazione analizza il sistema e cerca eventuali anomalie e danni presenti nelle impostazioni del browser e del sistema operativo. La diagnostica della protezione presenta diversi aspetti quali la ricerca di installazioni Rootkit (ovvero programmi per il monitoraggio segreto di un sistema violato da un hacker), la ricerca di servizi e impostazioni vulnerabili e la raccolta di informazioni su processi e driver.

La diagnostica del sistema alla ricerca di eventuali vulnerabilità può richiedere diversi minuti. Quando è completa, le informazioni raccolte vengono analizzate per valutare i problemi di protezione nell'ottica di una possibile minaccia al sistema.

Tutti i problemi rilevati durante la fase di analisi del sistema vengono raggruppati in base al livello di pericolo che presentano. Kaspersky Lab offre una serie di azioni per ciascun gruppo di problemi, che aiutano a eliminare le vulnerabilità e i punti deboli nelle impostazioni del sistema. Si tratta di tre gruppi di problemi distinti e, rispettivamente, tre gruppi di azioni a essi associate:

- *Le Azioni caldamente consigliate* aiutano a eliminare i problemi che costituiscono una grave minaccia. È consigliabile eseguire tutte le azioni appartenenti a questo gruppo.
- *Le Azioni consigliate* consentono di eliminare i problemi che costituiscono una minaccia potenziale. È consigliabile eseguire anche tutte le azioni appartenenti a questo gruppo.
- *Le Azioni aggiuntive* consentono di riparare i danni che non costituiscono una minaccia al momento ma che potrebbero minacciare la sicurezza del computer in futuro.

Il risultato della ricerca delle vulnerabilità potenziali nel sistema operativo e nelle applicazioni installate nel computer viene rappresentato da collegamenti diretti alle critical fix (aggiornamenti alle applicazioni).

Dopo l'avvio dell'attività di ricerca delle vulnerabilità (vedere pagina [85](#)), ne viene visualizzato lo stato di avanzamento nella finestra principale dell'applicazione e nella finestra **Scansione vulnerabilità**, nel campo **Fine**. Le vulnerabilità rilevate durante la scansione del sistema e delle applicazioni vengono visualizzate nella stessa finestra, nelle schede **Vulnerabilità di sistema** e **Applicazioni vulnerabili**.

Durante la ricerca di minacce, le informazioni sui risultati vengono registrate in un rapporto di Kaspersky Anti-Virus.

Nella sezione **Scansione vulnerabilità** della finestra delle impostazioni dell'applicazione, è possibile impostare una pianificazione iniziale (vedere pagina [86](#)) e creare un elenco di oggetti da sottoporre a scansione per un'attività di ricerca delle vulnerabilità (vedere pagina [85](#)), analogamente alle attività di scansione anti-virus. Per impostazione predefinita, le applicazioni già installate nel computer vengono selezionate come oggetti da esaminare.

VEDERE ANCHE:

Avvio dell'attività di ricerca delle vulnerabilità	85
Creazione di un collegamento per l'esecuzione di attività	85
Creazione di un elenco di oggetti da esaminare	85
Modalità di esecuzione: creazione di una pianificazione	86
Modalità di esecuzione: specifica di un account	87

AVVIO DELL'ATTIVITÀ DI RICERCA DELLE VULNERABILITÀ

L'attività di ricerca delle vulnerabilità può essere avviata nei modi seguenti:

- dalla finestra principale dell'applicazione (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [40](#));
- utilizzando un collegamento esistente (vedere pagina [85](#)).

Le informazioni sull'esecuzione dell'attività vengono visualizzate nella finestra principale di Kaspersky Anti-Virus e nella finestra **Scansione Vulnerabilità**.

➡ *Per avviare l'attività utilizzando un collegamento:*

1. Aprire la cartella in cui è stato creato un collegamento.
2. Avviare l'attività facendo doppio clic su un collegamento. Lo stato di avanzamento dell'attività verrà visualizzato nella finestra principale dell'applicazione.

➡ *Per avviare l'attività di ricerca delle vulnerabilità dalla finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Cliccare sul bottone **Apri la finestra della Scansione Vulnerabilità**.
4. Nella finestra visualizzata, cliccare sul bottone **Avvia Scansione Vulnerabilità**. Lo stato di avanzamento dell'esecuzione dell'attività verrà visualizzato nel campo **Fine**. Cliccare di nuovo sul bottone per interrompere l'esecuzione dell'attività.

CREAZIONE DI UN COLLEGAMENTO PER L'ESECUZIONE DI ATTIVITÀ

L'applicazione offre l'opportunità di creare un collegamento per un avvio rapido dell'attività di ricerca delle vulnerabilità. Ciò consente di avviare l'attività senza aprire la finestra principale dell'applicazione.

➡ *Per creare un collegamento per l'avvio dell'attività di ricerca delle vulnerabilità:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Nella parte destra della finestra, nella sezione **Esecuzione rapida delle attività di scansione**, cliccare sul bottone **Crea collegamento** accanto al nome dell'attività richiesta (**Scansione Vulnerabilità**).
4. Nella finestra che viene visualizzata specificare il percorso in cui salvare il collegamento. Per impostazione predefinita, il collegamento viene creato con il nome di un'attività nella cartella *Risorse del computer* dell'utente corrente.

CREAZIONE DI UN ELENCO DI OGGETTI DA ESAMINARE

L'attività di ricerca delle vulnerabilità si basa su un elenco predefinito personalizzato di oggetti da esaminare. Questi oggetti contengono il sistema operativo e i programmi installati nel computer. È anche possibile specificare altri oggetti da esaminare: oggetti del file system del computer, ad esempio unità logiche, **database delle posta** o altri tipi di oggetti, ad esempio le unità di rete.

Gli oggetti vengono visualizzati nell'elenco subito dopo essere stati aggiunti. Se si seleziona la casella ☒ **Includi sottocartelle** mentre si aggiunge un oggetto, la scansione verrà eseguita in modo ricorsivo. Gli oggetti aggiunti manualmente vengono anche sottoposti a una scansione anti-virus.

Per eliminare un oggetto dall'elenco, selezionarlo e cliccare sul collegamento **Elimina**.

Gli oggetti che appaiono nell'elenco per impostazione predefinita non possono essere modificati né eliminati.

Oltre a eliminare gli oggetti dall'elenco, è possibile anche ignorarli temporaneamente durante l'esecuzione di una scansione. A tal fine, selezionare l'oggetto dall'elenco e deselezionare la casella a sinistra del nome dell'oggetto.

Se l'ambito di scansione è vuoto o non contiene oggetti selezionati, l'attività di scansione non può essere avviata.

► Per creare l'elenco di oggetti per un'attività di ricerca delle vulnerabilità:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività **Scansione Vulnerabilità** nella sezione **Scansione**.
3. Nel blocco **Ambito della scansione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra **Scansione Vulnerabilità: elenco degli oggetti** visualizzata, creare l'elenco utilizzando i collegamenti **Aggiungi**, **Modifica**, **Elimina**. Per escludere temporaneamente un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella.

MODALITÀ DI ESECUZIONE: CREAZIONE DI UNA PIANIFICAZIONE

È possibile pianificare l'esecuzione automatica dell'attività di ricerca delle vulnerabilità.

L'impostazione principale riguarda l'intervallo di tempo tra gli avvii dell'attività.

Se per qualsiasi motivo non è possibile avviare l'attività, ad esempio perché all'ora prevista il computer era spento, è possibile configurare l'attività in modo che venga avviata automaticamente non appena possibile.

► Per modificare una pianificazione per le attività di scansione:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività **Scansione Vulnerabilità** nella sezione **Scansione**.
3. Nel blocco **Modalità di esecuzione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Pianifica**, selezionare l'opzione **Manualmente** per avviare un'attività di scansione quando lo si ritiene più opportuno. Per eseguire l'attività periodicamente, selezionare **Pianifica** e creare una pianificazione di avvio dell'attività.

► Per configurare l'avvio automatico delle attività ignorate:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività **Scansione Vulnerabilità** nella sezione **Scansione**.
3. Nel blocco **Modalità di esecuzione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Pianifica**, selezionare la casella ☒ **Esegui le attività rimandate**.

MODALITÀ DI ESECUZIONE: SPECIFICA DI UN ACCOUNT

È possibile specificare un account utilizzato dall'applicazione durante l'esecuzione di un'attività di ricerca delle vulnerabilità.

➡ *Per specificare un account:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare l'attività **Scansione Vulnerabilità** nella sezione **Scansione**.
3. Nel blocco **Modalità di esecuzione**, cliccare sul bottone **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Account utente**, selezionare la casella  **Esegui l'attività come**. Specificare il nome utente e la password.

AGGIORNAMENTO

Mantenere l'applicazione aggiornata è un requisito fondamentale per garantire l'affidabilità della protezione del computer. Poiché ogni giorno nascono nuovi virus, Trojan e software nocivi, è importante aggiornare regolarmente l'applicazione per proteggere costantemente i dati personali. Le informazioni sulle minacce e i metodi che consentono di neutralizzarle sono memorizzate nei database di Kaspersky Anti-Virus. L'aggiornamento tempestivo di tali database diventa quindi un'operazione fondamentale per garantire una protezione affidabile.

L'aggiornamento dell'applicazione viene scaricato e comporta l'installazione degli aggiornamenti seguenti nel computer:

- Database di Kaspersky Anti-Virus.

La protezione delle informazioni è basata su database contenenti le firme delle minacce e gli attacchi di rete, nonché i metodi per contrastarli. I componenti della protezione li utilizzano per rilevare e disinfettare gli oggetti pericolosi sul computer. I database vengono aggiornati ogni ora con nuove voci relative alle nuove minacce. È pertanto consigliabile aggiornarli regolarmente.

Oltre ai database di Kaspersky Anti-Virus, vengono aggiornati i driver di rete che consentono ai componenti dell'applicazione di intercettare il traffico di rete.

- Moduli dell'applicazione.

Oltre ai database di Kaspersky Anti-Virus, è possibile anche aggiornare i moduli del programma. I pacchetti di aggiornamento correggono le vulnerabilità dell'applicazione e aggiungono nuove funzionalità o migliorano quelle esistenti.

I server di aggiornamento di Kaspersky Lab rappresentano le sorgenti degli aggiornamenti principali per Kaspersky Anti-Virus.

Per scaricare dai server gli aggiornamenti disponibili è necessario disporre di una connessione Internet. Per impostazione predefinita, le impostazioni di connessione a Internet vengono determinate automaticamente. Se le impostazioni del server proxy non vengono determinate automaticamente, è possibile modificare manualmente le impostazioni di connessione.

Durante un aggiornamento, i moduli e i database dell'applicazione nel computer vengono confrontati con quelli dell'origine degli aggiornamenti. Se il computer dispone dell'ultima versione dei database e dei moduli dell'applicazione, viene visualizzata una finestra di notifica che conferma che la protezione del computer è aggiornata. Se i database e i moduli sul computer e sul server di aggiornamento sono diversi, l'applicazione scarica solo la parte incrementale degli aggiornamenti. Il fatto che non vengano scaricati tutti i database e i moduli determina un aumento significativo della velocità di copia dei file e una riduzione del traffico Internet.

Se i database sono obsoleti, le dimensioni del pacchetto di aggiornamento possono essere piuttosto grandi e aumentare ulteriormente il traffico in Internet (fino a diverse decine di MB).

Prima di aggiornare i database, Kaspersky Anti-Virus ne crea copie di backup che possono risultare utili nel caso in cui l'utente desideri eseguire il rollback a una versione precedente di un database.

L'opzione di rollback dell'aggiornamento potrebbe essere necessaria se, ad esempio, i database vengono danneggiati durante il processo di aggiornamento. È possibile eseguire facilmente il rollback alla versione precedente e cercare di aggiornare nuovamente i database.

Durante l'aggiornamento di Kaspersky Anti-Virus, la copia degli aggiornamenti recuperati può essere copiata in un'origine locale. Questo servizio consente di aggiornare i database e i moduli del programma su computer di rete per non intasare il traffico in Internet.

È anche possibile configurare l'avvio automatico dell'aggiornamento.

Nella sezione **Aggiornamenti** della finestra principale dell'applicazione sono contenute informazioni sullo stato corrente dei database di Kaspersky Anti-Virus:

- data e ora di rilascio;
- numero di record del database e relativa composizione;
- stato dei database (aggiornati, obsoleti o danneggiati).

È possibile visualizzare il rapporto di aggiornamento contenente tutte le informazioni relative agli eventi verificatisi durante l'esecuzione dell'attività di aggiornamento cliccando sul collegamento **Rapporti** nella parte superiore della finestra. Una panoramica sull'attività dei virus è disponibile nel sito Web www.kaspersky.com/it cliccando sul **collegamento relativo all'analisi dell'attività dei virus**.

IN QUESTA SEZIONE:

Avvio dell'aggiornamento.....	89
Rollback dell'ultimo aggiornamento	89
Selezione di una sorgente degli aggiornamenti.....	90
Utilizzo di un server proxy	91
Impostazioni internazionali	91
Azioni da eseguire dopo l'aggiornamento.....	91
Aggiornamento da una cartella locale	92
Modifica della modalità di esecuzione dell'attività di aggiornamento	93
Esecuzione degli aggiornamenti utilizzando un altro account utente	93

AVVIO DELL'AGGIORNAMENTO

È possibile avviare la procedura di aggiornamento in qualsiasi momento. Gli aggiornamenti vengono scaricati dalla sorgente degli aggiornamenti selezionata (vedere la sezione "Selezione di una sorgente degli aggiornamenti" a pagina [90](#)).

È possibile aggiornare Kaspersky Anti-Virus utilizzando uno dei due metodi supportati:

- dal menu di scelta rapida (vedere la sezione "Menu di scelta rapida" a pagina [39](#));
- dalla finestra principale dell'applicazione (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [40](#)).

Le informazioni sull'aggiornamento verranno visualizzate nella sezione **Aggiornamenti** della finestra principale dell'applicazione.

► Per avviare l'aggiornamento di Kaspersky Anti-Virus dal menu di scelta rapida:

1. Cliccare con il pulsante destro del mouse sull'icona nell'area di notifica della barra delle applicazioni.
2. Selezionare la voce **Aggiorna** dal menu a discesa.

► Per avviare l'aggiornamento di Kaspersky Anti-Virus dalla finestra principale dell'applicazione:

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Scegliere il bottone **Aggiorna**. Lo stato di avanzamento dell'attività verrà visualizzato nella finestra principale dell'applicazione.

ROLLBACK DELL'ULTIMO AGGIORNAMENTO

All'inizio del processo di aggiornamento, Kaspersky Anti-Virus crea una copia di backup dei moduli dell'applicazione e dei database correnti. In questo modo, se l'aggiornamento non riesce, il programma può continuare a funzionare utilizzando i database precedenti.

L'opzione di rollback è utile, ad esempio, se una parte dei database è stata danneggiata. I database locali possono essere danneggiati dall'utente o da un programma dannoso. Questo è possibile solo se il componente Auto-Difesa (vedere la sezione "Auto-difesa di Kaspersky Anti-Virus" a pagina [103](#)) di Kaspersky Anti-Virus è abilitato. È possibile riportare i database allo stato precedente e ritentare l'aggiornamento in un secondo momento.

➡ *Per eseguire il rollback alla versione precedente del database:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Cliccare sul bottone **Rollback ai database precedenti**.

SELEZIONE DI UNA SORGENTE DEGLI AGGIORNAMENTI

Per *sorgente degli aggiornamenti* si intende una risorsa contenente gli aggiornamenti per i database e i moduli di applicazione di Kaspersky Anti-Virus. Le sorgenti degli aggiornamenti possono essere server HTTP o FTP, cartelle locali o cartelle di rete.

La sorgente degli aggiornamenti principale è costituita dai server degli aggiornamenti di Kaspersky Lab. Si tratta di speciali siti Internet contenenti gli aggiornamenti disponibili per i database e i moduli di applicazione per tutti i prodotti Kaspersky Lab.

Se non è possibile accedere ai server degli aggiornamenti di Kaspersky Lab, ad esempio in assenza di una connessione a Internet, chiamare l'ufficio centrale di Kaspersky Lab al numero +7 (495) 797-87-00 o +7 (495) 645-79-39 per richiedere informazioni sui partner di Kaspersky Lab che possono fornire aggiornamenti in formato compresso su floppy o dischi ZIP.

È possibile copiare gli aggiornamenti da un disco rimovibile e caricarli su un sito FTP o HTTP oppure salvarli in una cartella locale o di rete.

Quando si ordinano gli aggiornamenti salvati su un supporto rimovibile, è necessario specificare se si desiderano anche gli aggiornamenti dei moduli dell'applicazione.

Per impostazione predefinita, l'elenco contiene solo i server degli aggiornamenti di Kaspersky Lab.

Se si seleziona una risorsa esterna alla LAN come sorgente degli aggiornamenti, è necessario disporre di una connessione a Internet per poter eseguire l'aggiornamento.

Se sono state selezionate più risorse come sorgenti dell'aggiornamento, Kaspersky Anti-Virus cerca di connettersi a esse una dopo l'altra a partire da quella che occupa la prima posizione dell'elenco e recupera gli aggiornamenti dalla prima disponibile.

➡ *Per scegliere una sorgente degli aggiornamenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Cliccare sul bottone **Impostazioni** nella sezione **Sorgente dell'aggiornamento**.
4. Nella finestra visualizzata, nella scheda **Sorgente**, cliccare sul collegamento **Aggiungi**.
5. Selezionare un sito FTP o HTTP oppure immetterne l'indirizzo IP, il nome simbolico o l'URL nella finestra **Sorgente degli aggiornamenti** visualizzata.

UTILIZZO DI UN SERVER PROXY

Se si utilizza un server proxy per connettersi a Internet, è necessario configurarne le impostazioni.

➡ *Per configurare il server proxy, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Cliccare sul bottone **Impostazioni** nella sezione **Sorgente dell'aggiornamento**.
4. Nella finestra visualizzata, nella scheda **Sorgente**, cliccare sul bottone **Server proxy**.
5. Modificare le impostazioni del server proxy nella finestra **Impostazioni del server proxy** visualizzata.

IMPOSTAZIONI INTERNAZIONALI

Se si utilizzano i server degli aggiornamenti di Kaspersky Lab come sorgente degli aggiornamenti, è possibile selezionare la posizione ottimale del server da cui scaricare i file. I server Kaspersky Lab sono dislocati in più paesi. La scelta del server più vicino consente di risparmiare tempo e accelerare il download degli aggiornamenti.

➡ *Per scegliere il server più vicino:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Cliccare sul bottone **Impostazioni** nella sezione **Sorgente dell'aggiornamento**.
4. Nella finestra visualizzata, nella scheda **Origine**, sezione **Impostazioni internazionali**, selezionare l'opzione  **Seleziona dall'elenco** e selezionare il paese più vicino alla propria località corrente nell'elenco a discesa.

Se si seleziona la casella  **Rileva automaticamente**, le informazioni sulla posizione verranno copiate dal registro del sistema operativo durante l'esecuzione dell'aggiornamento.

AZIONI DA ESEGUIRE DOPO L'AGGIORNAMENTO

Kaspersky Anti-Virus consente di specificare anche le azioni che verranno eseguite automaticamente dopo l'aggiornamento. È possibile eseguire le azioni seguenti:

- **Ripeti la scansione degli oggetti in Quarantena dopo l'aggiornamento.** L'area di quarantena contiene oggetti che sono stati contrassegnati dall'applicazione come sospetti o possibilmente infetti. È possibile che al termine dell'aggiornamento del database il prodotto riesca a riconoscere la minaccia in modo inequivocabile e neutralizzarla. Dopo l'aggiornamento del database, l'applicazione potrebbe essere in grado di identificare la minaccia ed eliminarla. Per questo motivo l'applicazione esegue la scansione degli oggetti in quarantena dopo ogni aggiornamento. La scansione potrebbe infatti modificarne lo stato e consentire quindi il ripristino di alcuni oggetti nelle posizioni precedenti in modo che l'utente possa continuare a utilizzarli.
- **Crea una copia degli aggiornamenti nella cartella.** Se i computer sono collegati in una rete LAN domestica, non è necessario scaricare e installare gli aggiornamenti individualmente su ciascuno di essi. È possibile utilizzare il servizio di distribuzione degli aggiornamenti per risparmiare larghezza di banda di rete, poiché il servizio garantisce che gli aggiornamenti vengono scaricati solo una volta.

➡ *Per esaminare i file in quarantena dopo la scansione:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Selezionare la casella ☒ **Ripeti la scansione degli oggetti in Quarantena dopo l'aggiornamento** nella sezione **Avanzate**.

AGGIORNAMENTO DA UNA CARTELLA LOCALE

La procedura di recupero degli aggiornamenti da una cartella locale viene organizzata nel modo seguente:

1. Uno dei computer della rete recupera un pacchetto di aggiornamento di Kaspersky Anti-Virus dai server degli aggiornamenti Web di Kaspersky Lab o da un server mirror che ospita un insieme corrente di aggiornamenti. Gli aggiornamenti recuperati vengono salvati in una cartella condivisa.
2. Per recuperare tali aggiornamenti, altri computer in rete accedono alla cartella condivisa.

➡ *Per abilitare la modalità di distribuzione degli aggiornamenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Selezionare la casella ☒ **Crea una copia degli aggiornamenti nella cartella** nella sezione **Avanzate** e specificare il percorso di una cartella pubblica in cui verranno copiati tutti gli aggiornamenti scaricati nel campo in basso. È inoltre possibile selezionare il percorso nella finestra di dialogo visualizzata dopo aver cliccato sul bottone **Sfoglia**.

➡ *Se si desidera che gli aggiornamenti vengano eseguiti dalla cartella ad accesso pubblico selezionata, eseguire queste azioni su tutti i computer della rete:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Cliccare sul bottone **Impostazioni** nella sezione **Sorgente dell'aggiornamento**.
4. Nella finestra visualizzata, nella scheda **Sorgente**, cliccare sul collegamento **Aggiungi**.
5. Nella finestra **Sorgente degli aggiornamenti** visualizzata, selezionare una cartella o immetterne il percorso completo nel campo **Sorgente**.
6. Deselezionare la casella ☒ **Server degli aggiornamenti di Kaspersky Lab** nella scheda **Sorgente**.

MODIFICA DELLA MODALITÀ DI ESECUZIONE DELL'ATTIVITÀ DI AGGIORNAMENTO

La modalità di avvio dell'attività di aggiornamento di Kaspersky Anti-Virus viene selezionata durante la configurazione guidata dell'applicazione (vedere la sezione "Passaggio 3. Configurazione dell'aggiornamento dell'applicazione" a pagina [29](#)). Se si desidera modificare la modalità di avvio dell'aggiornamento selezionata, è possibile riconfigurarla.

L'attività di aggiornamento può essere avviata tramite una delle seguenti modalità:

-  **Automaticamente.** Kaspersky Anti-Virus verifica a intervalli specificati la disponibilità di nuovi aggiornamenti nella sorgente degli aggiornamenti. La frequenza della scansione può essere aumentata durante le epidemie e ridotta nei periodi più tranquilli. I nuovi aggiornamenti rilevati vengono scaricati e installati nel computer.
-  **In base alla pianificazione** (l'intervallo di tempo cambia in base alle impostazioni). Gli aggiornamenti vengono eseguiti automaticamente in base alla pianificazione creata.
-  **Manualmente.** Se si seleziona questa opzione, gli aggiornamenti di Kaspersky Anti-Virus verranno eseguiti manualmente.

➡ *Per configurare la pianificazione di avvio dell'attività di aggiornamento:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Cliccare sul bottone **Impostazioni** nella sezione **Modalità di esecuzione**.
4. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, selezionare la modalità di avvio dell'attività di aggiornamento nella sezione **Pianifica**. Se l'opzione  **In base alla pianificazione** è selezionata, creare la pianificazione.

Se per qualsiasi motivo un aggiornamento viene saltato, ad esempio perché all'ora prevista il computer era spento, è possibile configurare l'attività in modo che inizi automaticamente non appena possibile. A tale scopo, è sufficiente selezionare la casella  **Esegui le attività rimandate** nella parte inferiore della finestra. Questa casella di controllo è disponibile per tutte le opzioni di pianificazione, ad eccezione di **Ore**, **Minuti** e **Dopo l'avvio dell'applicazione**.

ESECUZIONE DEGLI AGGIORNAMENTI UTILIZZANDO UN ALTRO ACCOUNT UTENTE

Per impostazione predefinita, la procedura di aggiornamento viene eseguita utilizzando il proprio account utente. Tuttavia, Kaspersky Anti-Virus può eseguire l'aggiornamento da un'origine per la quale non si dispone di diritti di accesso, ad esempio una cartella di rete contenente aggiornamenti, o di credenziali utente di un proxy autorizzato. È possibile eseguire l'aggiornamento dell'applicazione utilizzando l'account di un utente che dispone dei diritti necessari.

➡ *Per avviare l'aggiornamento utilizzando un altro account utente:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Cliccare sul bottone **Impostazioni** nella sezione **Modalità di esecuzione**.
4. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Utente**, selezionare la casella  **Esegui l'attività come**. Specificare il nome utente e la password.

CONFIGURAZIONE IMPOSTAZIONI APPLICAZIONE

La finestra delle impostazioni dell'applicazione consente di accedere rapidamente alle principali impostazioni di Kaspersky Anti-Virus.

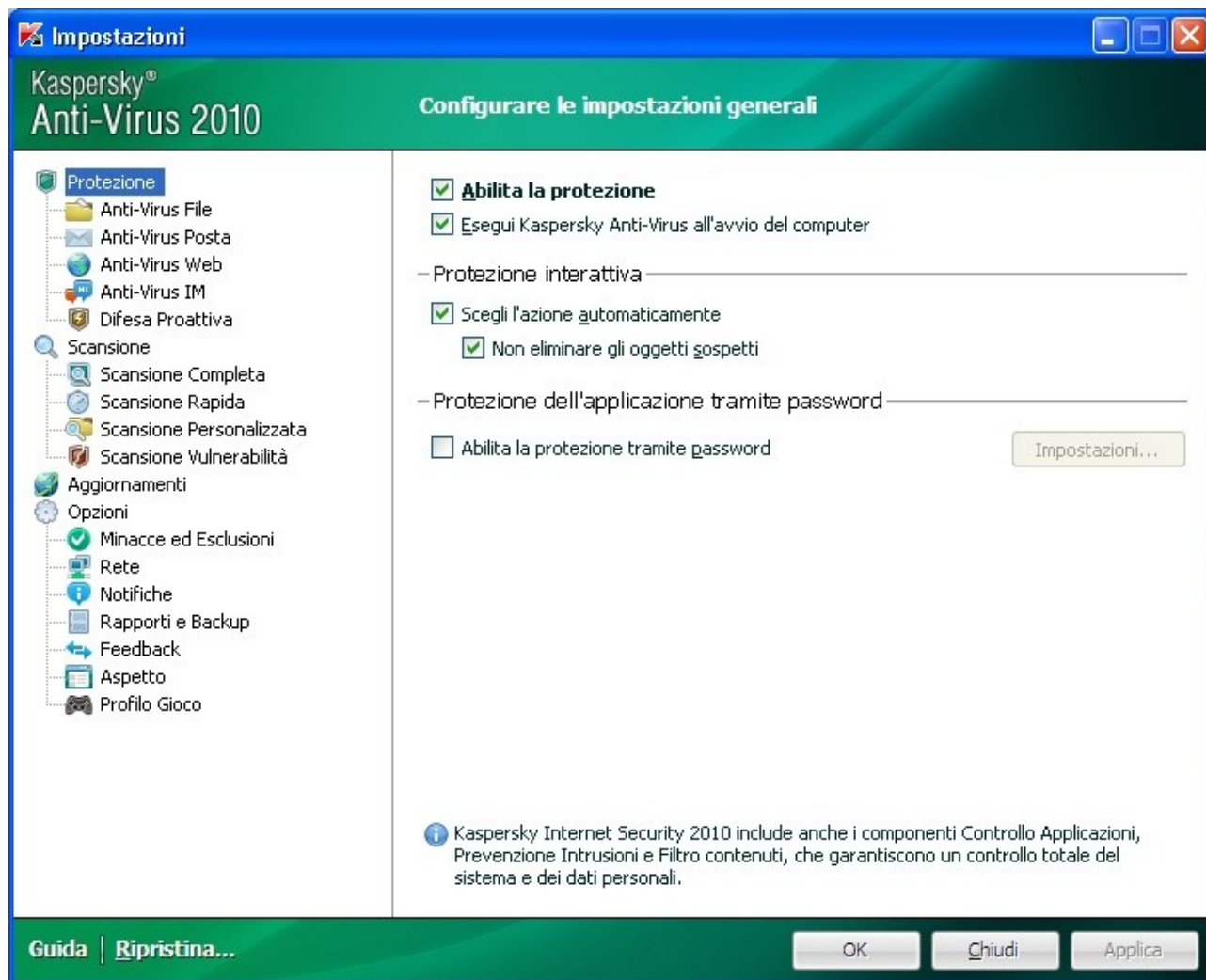


Figura 11. finestra delle impostazioni dell'applicazione

La finestra delle impostazioni si compone di due parti:

- La parte sinistra consente di accedere ai componenti di Kaspersky Anti-Virus, alle attività di scansione anti-virus, alle attività di aggiornamento e così via.
- La parte destra della finestra contiene un elenco di impostazioni relative, ad esempio, al componente e all'attività selezionati nella parte sinistra della finestra.

È possibile aprire questa finestra:

- Dalla finestra principale dell'applicazione (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [40](#)). A tale scopo, cliccare sul collegamento **Impostazioni** nella parte superiore della finestra principale.

- Dal menu di scelta rapida (vedere la sezione "Menu di scelta rapida" a pagina [39](#)). A tale scopo, selezionare la voce **Impostazioni** dal menu di scelta rapida dell'applicazione.



Figura 12. Menu di scelta rapida

IN QUESTA SEZIONE:

Protezione	95
Anti-Virus File	98
Anti-Virus Posta	99
Anti-Virus Web	99
Anti-Virus IM	100
Difesa Proattiva	101
Scansione	101
Aggiornamento	102
Impostazioni	103

PROTEZIONE

Nella finestra **Protezione** è possibile utilizzare le funzioni avanzate di Kaspersky Anti-Virus elencate di seguito:

- Abilitazione/disabilitazione della protezione di Kaspersky Anti-Virus (vedere pagina [95](#)).
- Avvio di Kaspersky Anti-Virus all'avvio del sistema operativo (vedere pagina [96](#)).
- Utilizzo della modalità di protezione interattiva (vedere pagina [96](#)).
- Restrizione dell'accesso a Kaspersky Anti-Virus (vedere pagina [97](#)).

ABILITAZIONE/DISABILITAZIONE DELLA PROTEZIONE DEL COMPUTER

Per impostazione predefinita, Kaspersky Anti-Virus viene avviato durante il caricamento del sistema operativo e protegge il computer finché non viene spento. Tutti i componenti di protezione sono in esecuzione.

La protezione offerta da Kaspersky Anti-Virus può essere abilitata completamente o parzialmente.

Gli esperti di Kaspersky Lab consigliano di **non disabilitare la protezione**, in quanto questo può portare all'infezione del computer e alla perdita di dati.

Quando la protezione è disabilitata, tutti i componenti diventano inattivi. Vengono utilizzati i segni seguenti:

- icona inattiva (grigia) (vedere la sezione "Icona dell'area di notifica" a pagina [38](#)) nell'area di notifica della barra delle applicazioni;
- colore rosso dell'indicatore di protezione.

In questo caso, la protezione è descritta nel contesto dei componenti di protezione. Disabilitare o sospendere i componenti di protezione non pregiudica le prestazioni delle attività di scansione anti-virus e degli aggiornamenti di Kaspersky Anti-Virus.

➡ *Per disabilitare completamente la protezione:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Protezione**.
3. Deselezionare la casella ☒ **Abilita la protezione**.

AVVIO DI KASPERSKY ANTI-VIRUS ALL'AVVIO DEL SISTEMA OPERATIVO

Se è necessario arrestare completamente Kaspersky Anti-Virus per qualsiasi motivo, selezionare la voce **Esci** dal menu di scelta rapida (vedere la sezione "Menu di scelta rapida" a pagina [39](#)) di Kaspersky Anti-Virus. L'applicazione non viene più caricata nella RAM. Ciò significa che il computer viene eseguito senza protezione.

È possibile riabilitare la protezione del computer caricando Kaspersky Anti-Virus dal menu **Start** → **Programmi** → **Kaspersky Anti-Virus 2010** → **Kaspersky Anti-Virus 2010**.

La protezione può essere anche ripresa automaticamente dopo aver riavviato il sistema operativo.

➡ *Per abilitare questa modalità:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Protezione**.
3. Selezionare la casella ☒ **Esegui Kaspersky Anti-Virus all'avvio del computer**.

UTILIZZO DELLA MODALITÀ DI PROTEZIONE INTERATTIVA

Kaspersky Anti-Virus interagisce con l'utente in due modi:

- *Modalità di protezione interattiva.* Kaspersky Anti-Virus notifica all'utente tutti gli eventi pericolosi o sospetti che si verificano nel sistema, lasciandogli la libertà di scegliere se consentire o bloccare le azioni.
- *Modalità di protezione automatica.* Kaspersky Anti-Virus applica automaticamente le azioni raccomandate dagli esperti di Kaspersky Lab in risposta al verificarsi di eventi pericolosi.

► *Per utilizzare la modalità di protezione automatica:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Protezione**.
3. Nella sezione **Protezione interattiva**, selezionare la casella ☒ **Scegli l'azione automaticamente**. Se non si desidera che Kaspersky Anti-Virus elimini gli oggetti sospetti durante l'esecuzione in modalità automatica, selezionare la casella ☒ **Non eliminare gli oggetti sospetti**.

LIMITAZIONE DELL'ACCESSO A KASPERSKY ANTI-VIRUS

Un personal computer può essere utilizzato da diversi utenti, con differenti livelli di esperienza in ambito informatico. Se si consente il libero accesso a Kaspersky Anti-Virus e alle relative impostazioni, il livello di protezione generale del computer potrebbe diminuire drasticamente.

Per aumentare il livello di protezione del computer, utilizzare una password per accedere a Kaspersky Anti-Virus. È possibile bloccare qualsiasi operazione di Kaspersky Anti-Virus, ad eccezione delle notifiche relative al rilevamento di oggetti pericolosi, o impedire l'esecuzione delle azioni seguenti:

- modifica delle impostazioni dell'applicazione;
- chiusura dell'applicazione.

► *Per proteggere l'accesso a Kaspersky Anti-Virus mediante una password, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Protezione**.
3. Nella sezione **Protezione dell'applicazione tramite password**, selezionare la casella ☒ **Abilita la protezione tramite password** e cliccare sul bottone **Impostazioni**.
4. Nella finestra **Protezione dell'applicazione tramite password** visualizzata, immettere la password e specificare l'area coperta dalla limitazione di accesso. In questo modo, ogni volta che un utente del computer cercherà di eseguire le azioni selezionate dovrà immettere una password.

ANTI-VIRUS FILE

In questa finestra sono raggruppate le impostazioni del componente Anti-Virus File (vedere la sezione "Protezione del file system del computer" a pagina [43](#)). Modificando le impostazioni è possibile eseguire le azioni seguenti:

- disabilitare Anti-Virus File;
- modificare il livello di protezione (vedere pagina [45](#));
- modificare l'azione da eseguire sugli oggetti rilevati (vedere pagina [45](#));
- creare un ambito di protezione (vedere pagina [46](#));
- ottimizzare la scansione (vedere pagina [48](#));
- configurare la scansione dei file compositi (vedere pagina [48](#));
- modificare la modalità di scansione (vedere pagina [49](#));
- utilizzare l'analisi euristica (vedere pagina [47](#));
- sospendere il componente (vedere pagina [50](#));
- selezionare una tecnologia di scansione (vedere pagina [50](#));
- ripristinare le impostazioni di protezione predefinite (vedere pagina [52](#)) se sono state modificate.

➡ *Per disabilitare Anti-Virus File, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Deselezionare la casella ☒ **Abilita Anti-Virus File** nella parte destra della finestra.

➡ *Per passare alle impostazioni di Anti-Virus File, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella sezione **Protezione** della finestra visualizzata, selezionare il componente **Anti-Virus File**.
3. Nella parte destra della finestra, selezionare le impostazioni del componente relative al livello di protezione e alla reazione alle minacce. Cliccare sul bottone **Impostazioni** per visualizzare le altre impostazioni di Anti-Virus File.

ANTI-VIRUS POSTA

In questa finestra sono raggruppate le impostazioni del componente Anti-Virus Posta (vedere la sezione "Protezione della posta" a pagina [53](#)). Modificando le impostazioni è possibile eseguire le azioni seguenti:

- disabilitare Anti-Virus Posta;
- modificare il livello di protezione (vedere pagina [54](#));
- modificare l'azione da eseguire sugli oggetti rilevati (vedere pagina [55](#));
- creare un ambito di protezione (vedere pagina [56](#));
- utilizzare l'analisi euristica (vedere pagina [58](#));
- configurare la scansione dei file composti (vedere pagina [58](#));
- configurare il filtraggio degli oggetti allegati al messaggio di posta elettronica (vedere pagina [59](#));
- ripristinare le impostazioni di protezione della posta elettronica (vedere pagina [59](#)).

➡ *Per disabilitare Anti-Virus Posta, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Posta**.
3. Deselezionare la casella ☒ **Abilita Anti-Virus Posta** nella parte destra della finestra.

➡ *Per passare alle impostazioni di Anti-Virus Posta, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Posta**.
3. Nella parte destra della finestra, selezionare le impostazioni del componente relative al livello di protezione e alla reazione alle minacce. Cliccare sul bottone **Impostazioni** per visualizzare le altre impostazioni di Anti-Virus Posta.

ANTI-VIRUS WEB

In questa finestra sono raggruppate le impostazioni del componente Anti-Virus Web (vedere la sezione "Protezione del traffico Web" a pagina [60](#)). Modificando le impostazioni è possibile eseguire le azioni seguenti:

- disabilitare Anti-Virus Web;
- modificare il livello di protezione (vedere pagina [62](#));
- modificare l'azione da eseguire sugli oggetti rilevati (vedere pagina [62](#));
- creare un ambito di protezione (vedere pagina [63](#));
- modificare i metodi di scansione (vedere pagina [63](#));
- utilizzare la barra degli strumenti degli URL di Kaspersky (vedere pagina [64](#));
- ottimizzare la scansione (vedere pagina [66](#));
- utilizzare l'analisi euristica (vedere pagina [65](#));
- ripristinare le impostazioni predefinite di Anti-Virus Web (vedere pagina [66](#)).

➡ *Per disabilitare Anti-Virus Web, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Deselezionare la casella ☒ **Abilita Anti-Virus Web** nella parte destra della finestra.

➡ *Per passare alle impostazioni di Anti-Virus Web, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.
3. Nella parte destra della finestra, selezionare le impostazioni del componente relative al livello di protezione e alla reazione alle minacce. Cliccare sul bottone **Impostazioni** per visualizzare le altre impostazioni di Anti-Virus Web.

ANTI-VIRUS IM

In questa finestra sono raggruppate le impostazioni del componente Anti-Virus IM (vedere la sezione "Protezione del traffico dei programmi di messaggistica istantanea" a pagina [67](#)). Modificando le impostazioni è possibile eseguire le azioni seguenti:

- disabilitare Anti-Virus IM;
- creare un ambito di protezione (vedere pagina [68](#));
- modificare il metodo di scansione (vedere pagina [68](#));
- utilizzare l'analisi euristica (vedere pagina [69](#)).

➡ *Per disabilitare Anti-Virus IM, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus IM**.
3. Deselezionare la casella ☒ **Abilita Anti-Virus IM** nella parte destra della finestra.

➡ *Per passare alle impostazioni di Anti-Virus IM, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus IM**.
3. Nella parte destra della finestra, modificare le impostazioni del componente nel modo desiderato.

DIFESA PROATTIVA

In questa finestra sono raggruppate le impostazioni del componente Difesa Proattiva. Modificando le impostazioni è possibile eseguire le azioni seguenti:

- disabilitare Difesa Proattiva;
- gestire l'elenco di attività pericolose;
- modificare la reazione dell'applicazione alle attività pericolose nel sistema (vedere pagina [71](#));
- creare un gruppo di applicazioni attendibili (vedere pagina [72](#));
- monitorare gli account utente del sistema (vedere pagina [72](#)).

➡ *Per disabilitare Difesa Proattiva, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
3. Deselezionare la casella ☒ **Abilita Difesa Proattiva** a destra della finestra.

➡ *Per procedere alla modifica delle impostazioni di Difesa Proattiva, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
3. Nella parte destra della finestra, modificare le impostazioni del componente nel modo desiderato.

SCANSIONE

La selezione del metodo da utilizzare per la scansione degli oggetti presenti nel computer viene determinata dal set di proprietà assegnato a ogni attività.

Kaspersky Lab distingue tra attività di scansione anti-virus e attività di ricerca delle vulnerabilità. Le attività di scansione anti-virus includono quanto segue:

- **Scansione Personalizzata.** Scansione degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi oggetto nel file system del computer.
- **Scansione Completa.** Una scansione approfondita dell'intero sistema. Per impostazioni predefinite, vengono sottoposti a scansione gli oggetti seguenti: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di messaggi e-mail, dischi fissi, supporti di archiviazione rimovibili e unità di rete.
- **Scansione Rapida.** Scansione anti-virus degli oggetti di avvio del sistema operativo.

È possibile eseguire le azioni seguenti nella finestra delle impostazioni di ogni attività anti-virus:

- selezionare il livello di protezione con le impostazioni correlate definendo il comportamento dell'attività in fase di runtime;
- selezionare l'azione che verrà eseguita dall'applicazione al rilevamento di un oggetto infetto/potenzialmente infetto;
- creare una pianificazione per eseguire le attività automaticamente;
- creare un elenco di oggetti da sottoporre a scansione (per le attività di scansione rapida e scansione completa);
- specificare i tipi di file da esaminare per la ricerca di virus;
- specificare le impostazioni di scansione per i file composti;
- selezionare i metodi di scansione e le tecnologie di scansione.

Nella sezione **Scansione** è possibile specificare le impostazioni per la scansione automatica delle unità rimovibili quando vengono connesse al computer nonché creare collegamenti per l'avvio rapido delle attività di scansione anti-virus e di scansione delle vulnerabilità.

Nella finestra delle impostazioni, è possibile eseguire le azioni seguenti per un'attività di ricerca delle vulnerabilità:

- creare una pianificazione per eseguire le attività automaticamente;
- creare un elenco di oggetti da sottoporre a scansione.

➡ *Per modificare le impostazioni delle attività:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione (Scansione Completa, Scansione Rapida, Scansione Personalizzata, Scansione Vulnerabilità)**.
3. Nella parte destra della finestra, configurare le impostazioni.

AGGIORNAMENTO

L'aggiornamento di Kaspersky Anti-Virus viene eseguito in base all'insieme di parametri.

Nella finestra di configurazione dell'attività di aggiornamento è possibile eseguire le azioni seguenti:

- modificare l'indirizzo della risorsa dalla quale verranno distribuiti e installati gli aggiornamenti delle applicazioni;
- specificare il tipo di modalità in base al quale verrà avviato il processo di aggiornamento dell'applicazione;
- impostare la pianificazione per l'esecuzione di un'attività;
- specificare l'account con il quale avviare l'aggiornamento;
- selezionare le azioni da eseguire al termine dell'aggiornamento dell'applicazione.

➡ *Per procedere alla configurazione dell'aggiornamento:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
3. Selezionare la modalità di esecuzione richiesta nella parte destra della finestra e selezionare un'origine di aggiornamento. Configurare altre impostazioni dell'attività nella sezione **Avanzate**.

IMPOSTAZIONI

Nella finestra **Protezione** è possibile utilizzare le funzioni avanzate di Kaspersky Anti-Virus elencate di seguito:

- Auto-difesa di Kaspersky Anti-Virus (vedere pagina [103](#)).
- Utilizzo della tecnologia di disinfezione avanzata (vedere pagina [104](#)).
- Servizio di risparmio energetico per il funzionamento a batteria (vedere pagina [104](#)).
- Rinvio dell'esecuzione dell'attività di scansione anti-virus quando comporta un rallentamento di altre applicazioni (vedere pagina [104](#)).
- Esportazione/importazione delle impostazioni di Kaspersky Anti-Virus (vedere pagina [105](#)).
- Ripristino delle impostazioni predefinite di Kaspersky Anti-Virus (vedere pagina [105](#)).

AUTO-DIFESA DI KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus garantisce la protezione del computer da programmi malware e, proprio per questo, può essere essa stessa oggetto di attacchi da parte di tali programmi che cercano di bloccare l'attività o eliminarla.

Per garantire l'affidabilità del sistema di protezione del computer, Kaspersky Anti-Virus include anche funzionalità di auto-protezione e di protezione dall'accesso remoto.

Nei computer che utilizzano sistemi operativi a 64 bit e Microsoft Windows Vista, l'autodifesa di Kaspersky Anti-Virus è disponibile solo per impedire la modifica o l'eliminazione dei file del programma sui dischi locali e le relative voci del registro di sistema.

Accade di frequente che programmi di amministrazione remota come RemoteAdmin siano necessari durante l'utilizzo della protezione da accessi remoti. Per garantire il normale funzionamento, è necessario aggiungere questi programmi all'elenco di applicazioni attendibili e abilitare l'impostazione **Non monitorare l'attività dell'applicazione** per ciascuna di esse.

➡ *Per abilitare i meccanismi di auto-difesa di Kaspersky Anti-Virus, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Opzioni**.
3. Nella sezione **Auto-Difesa**, selezionare la casella ☒ **Abilita Auto-Difesa** per distribuire il meccanismo di protezione di Kaspersky Anti-Virus dalle modifiche o dall'eliminazione dei file del disco rigido, dei processi della RAM e delle voci del registro di sistema.

Nella sezione **Auto-Difesa**, selezionare la casella ☒ **Disabilita il servizio di controllo esterno** per bloccare qualsiasi tentativo di gestire i servizi dell'applicazione in remoto.

Se si tenta di eseguire una delle azioni elencate, verrà visualizzato un messaggio sopra l'icona dell'applicazione nell'area di notifica della barra delle applicazioni (sempre che il servizio di notifica non sia stato disabilitato dall'utente).

TECNOLOGIA AVANZATA DI DISINFEZIONE

I programmi dannosi moderni possono invadere i livelli più bassi di un sistema operativo, il che li rende praticamente impossibile da rilevare. Quando l'attività dannosa viene rilevata nel sistema, Kaspersky Anti-Virus consente di eseguire una procedura avanzata di disinfezione che rende possibile l'eliminazione della minaccia dal computer.

In seguito a questa procedura, è necessario riavviare il computer. Dopo aver riavviato il computer, viene consigliata l'esecuzione di una scansione anti-virus completa.

➡ *Per avviare la procedura avanzata di disinfezione, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Opzioni**.
3. Nella sezione **Compatibilità** selezionare la casella ☒ **Abilita la tecnologia avanzata di disinfezione**.

UTILIZZO DI KASPERSKY ANTI-VIRUS SU UN COMPUTER PORTATILE

Per risparmiare energia su un computer portatile, è possibile rimandare le attività di scansione anti-virus.

Poiché sia la scansione anti-virus che l'aggiornamento richiedono una notevole quantità di risorse e di tempo, è consigliabile disabilitare l'avvio pianificato di tali attività. In questo modo si prolunga la durata della batteria. Se necessario, è possibile aggiornare Kaspersky Anti-Virus o avviare una scansione anti-virus manuale.

➡ *Per utilizzare il servizio di risparmio energetico per funzionamento a batteria, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Opzioni**.
3. Nella sezione **Compatibilità**, selezionare la casella ☒ **Disabilita le scansioni programmate durante l'alimentazione a batteria**.

PRESTAZIONI DEL COMPUTER DURANTE L'ESECUZIONE DELLE ATTIVITÀ

È possibile posticipare le attività di scansione anti-virus per limitare il carico sulla CPU (Central Processing Unit) e sui sottosistemi di archiviazione su disco.

L'esecuzione di attività di scansione aumenta il carico sulla CPU e sui sottosistemi del disco, con conseguente rallentamento dell'esecuzione delle altre applicazioni. In questi casi, per impostazione predefinita Kaspersky Anti-Virus sospende l'esecuzione delle attività anti-virus e libera le risorse di sistema per le applicazioni dell'utente.

Alcune applicazioni, tuttavia, verranno avviate immediatamente dopo il rilascio delle risorse della CPU e verranno eseguite in background. Per fare in modo che la scansione non dipenda dalle prestazioni di tali applicazioni, è consigliabile evitare di assegnare a queste risorse del sistema.

Si noti che questa impostazione può essere configurata individualmente per ciascuna attività di scansione. In questo caso, la configurazione di un'attività specifica ha una priorità più alta.

➡ *Per posticipare l'esecuzione di un'attività di scansione anti-virus quando rallenta altri programmi:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Opzioni**.
3. Nella sezione **Compatibilità**, selezionare la casella ☒ **Concedi risorse alle altre applicazioni**.

ESPORTAZIONE/IMPORTAZIONE DELLE IMPOSTAZIONI DI KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus offre la possibilità di importare ed esportare le proprie impostazioni.

Questa funzione è utile, ad esempio, quando Kaspersky Anti-Virus è installato sia nel computer di casa che in quello dell'ufficio. È possibile configurare le impostazioni preferite del programma sul computer di casa, esportarle sotto forma di file su un disco e, servendosi della funzione di importazione, caricarle sul computer in ufficio. Le impostazioni vengono salvate in uno speciale file di configurazione.

➡ *Per esportare le impostazioni correnti di Kaspersky Anti-Virus, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Opzioni**.
3. Nella sezione **Gestione delle impostazioni dell'applicazione** cliccare sul bottone **Salva**.
4. Nella finestra visualizzata, immettere il nome del file di configurazione e il percorso in cui salvarlo.

➡ *Per importare le impostazioni dell'applicazione da un file di configurazione salvato:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Opzioni**.
3. Nella sezione **Gestione delle impostazioni dell'applicazione** cliccare sul bottone **Carica**.
4. Nella finestra visualizzata, selezionare il file da cui importare le impostazioni di Kaspersky Anti-Virus.

RIPRISTINO DELLE IMPOSTAZIONI PREDEFINITE

È sempre possibile ripristinare le impostazioni predefinite o consigliate di Kaspersky Anti-Virus. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Le impostazioni predefinite vengono ripristinate mediante la Configurazione guidata dell'applicazione (vedere la sezione "Configurazione guidata dell'applicazione" a pagina [26](#)).

Nella finestra visualizzata, verrà chiesto di stabilire quali impostazioni salvare durante il ripristino del livello di protezione consigliato e per quali componenti.

L'elenco contiene i componenti di Kaspersky Anti-Virus le cui impostazioni sono state modificate dall'utente. Se sono state create impostazioni speciali per uno o più componenti, anche queste verranno visualizzate nell'elenco.

Tali elenchi vengono creati durante l'utilizzo di Kaspersky Anti-Virus in base alle singole attività e ai requisiti di protezione. La relativa creazione può richiedere molto tempo, pertanto si consiglia di salvarli prima di ripristinare le impostazioni predefinite dell'applicazione.

Al termine della Configurazione guidata, viene impostato il livello di protezione **Consigliato** per tutti i componenti, tranne che per le impostazioni che si è deciso di mantenere personalizzate durante il ripristino. Verranno inoltre applicate le impostazioni specificate durante l'esecuzione della procedura guidata.

➡ *Per ripristinare le impostazioni relative alla protezione, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Opzioni**.
3. Nella sezione **Gestione delle impostazioni dell'applicazione** cliccare sul bottone **Ripristina**.
4. Nella finestra visualizzata, selezionare le caselle relative alle impostazioni da salvare. Cliccare sul bottone **Avanti**. La Configurazione guidata dell'applicazione verrà eseguita. Seguirne le istruzioni.

MINACCE ED ESCLUSIONI

Nella sezione **Minacce ed Esclusioni** della finestra delle impostazioni di Kaspersky Anti-Virus è possibile eseguire le azioni seguenti:

- selezionare le categorie di minacce rilevabili (vedere la sezione "Selezione delle categorie di minacce rilevabili" a pagina [107](#));
- creare l'area attendibile per l'applicazione.

L'*area attendibile* è un elenco di oggetti creato dall'utente che non dovrebbe essere controllato dall'applicazione. In altre parole, si tratta di un insieme di esclusioni dall'ambito di protezione di Kaspersky Anti-Virus.

L'area attendibile viene creata in base all'elenco di applicazioni attendibili (vedere la sezione "Selezione delle applicazioni attendibili" a pagina [107](#)) e alle regole di esclusione (vedere la sezione "Regole di esclusione" a pagina [108](#)).

L'utente crea un'area attendibile sulla base delle caratteristiche degli oggetti che utilizza e delle applicazioni installate nel computer. Questo elenco di esclusioni può tornare utile, ad esempio, se l'applicazione blocca l'accesso a un oggetto o programma della cui sicurezza l'utente è assolutamente certo.

VEDERE ANCHE:

Selezione delle categorie di minacce rilevabili	107
Selezione delle applicazioni attendibili	107
Regole di esclusione	108
Ulteriori impostazioni di esclusione.....	108
Maschere di esclusione file consentite	109
Maschere dei tipi di minaccia consentiti	109

SELEZIONE DELLE CATEGORIE DI MINACCE RILEVABILI

Kaspersky Anti-Virus protegge da diversi tipi di programmi pericolosi. A prescindere dalle impostazioni selezionate, l'applicazione esegue sempre la scansione e la disinfezione per eliminare virus, Trojan e utilità di hacking. Questi programmi infatti possono danneggiare gravemente il computer. Per offrire una maggiore protezione al computer, è possibile ampliare l'elenco di minacce da rilevare, abilitando il controllo di vari programmi potenzialmente pericolosi.

► *Per selezionare le categorie di minacce rilevabili, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Minacce ed Esclusioni**. Cliccare sul bottone **Impostazioni** nella sezione **Minacce**.
3. Nella finestra **Minacce** visualizzata, selezionare le categorie di minacce da cui si desidera proteggere il computer.

SELEZIONE DELLE APPLICAZIONI ATTENDIBILI

È possibile creare un elenco delle applicazioni attendibili che impedirà il controllo delle relative attività di rete e dei file, incluse quelle sospette, nonché dei relativi tentativi di accedere al registro di sistema.

È ad esempio possibile ritenere che gli oggetti utilizzati in Blocco note di Microsoft Windows siano sicuri e non necessitino di scansione. In altre parole, si considera affidabile quest'applicazione. Per escludere dalla scansione gli oggetti utilizzati da questo processo, aggiungere l'applicazione Blocco note all'elenco delle applicazioni attendibili. Il file eseguibile e il processo dell'applicazione attendibile saranno contemporaneamente sottoposti a scansione anti-virus come in precedenza. Per escludere completamente un'applicazione dalla scansione, è consigliabile utilizzare le regole di esclusione.

Inoltre, determinate azioni classificate come pericolose potrebbero essere ritenute normali da diverse applicazioni. Le applicazioni che ad esempio commutano automaticamente le tastiere, come Punto Switcher, intercettano regolarmente il testo immesso sulla tastiera. Per tenere conto delle caratteristiche specifiche di tali applicazioni e disabilitare il monitoraggio delle relative attività, è consigliabile aggiungerle all'elenco delle applicazioni attendibili.

L'esclusione delle applicazioni attendibili dalla scansione consente di risolvere eventuali problemi di compatibilità dell'applicazione con altri programmi, ad esempio il problema della doppia scansione del traffico di rete di un computer di terze parti da parte di Kaspersky Anti-Virus e di un'altra applicazione anti-virus, nonché di aumentare la velocità delle prestazioni del computer, aspetto di fondamentale importanza quando si utilizzano applicazioni server.

Per impostazione predefinita, Kaspersky Anti-Virus esamina gli oggetti aperti, eseguiti o salvati da qualsiasi processo di programma e monitora l'attività di tutte le applicazioni e il traffico di rete che creano.

► *Per aggiungere un'applicazione all'elenco delle applicazioni attendibili, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Minacce ed Esclusioni**.
3. Nella sezione **Esclusioni**, cliccare sul bottone **Impostazioni**.
4. Nella finestra visualizzata, nella scheda **Applicazioni attendibili**, cliccare sul collegamento **Aggiungi**.
5. Nel menu visualizzato, selezionare un'applicazione. Quando si seleziona la voce **Sfoglia**, viene aperta una finestra nella quale è necessario specificare il percorso di un file eseguibile. Quando si seleziona la voce **Applicazioni**, viene aperto l'elenco di applicazioni attualmente in esecuzione.
6. Nella finestra **Esclusioni per le applicazioni** visualizzata, specificare le impostazioni delle regole per l'applicazione.

L'applicazione affidabile può essere cambiata o eliminata dall'elenco tramite i corrispondenti collegamenti nella parte inferiore della scheda. Per rimuovere un'applicazione dall'elenco senza eliminarla, deselezionare la casella in corrispondenza del nome.

REGOLE DI ESCLUSIONE

Il software potenzialmente pericoloso non svolge una funzione dannosa vera e propria ma può essere utilizzato dagli hacker come componente ausiliario di un codice maligno in quanto contiene errori e vulnerabilità. Questa categoria include, ad esempio, programmi di amministrazione remota, client IRC, server ftp, utilità multiuso per arrestare o nascondere processi, keylogger, password cracker, autodialer e così via. Tali programmi non sono classificati come virus (not-a-virus). Essi possono essere suddivisi in diversi tipi, quali Adware, Joke, Riskware e così via. Per ulteriori informazioni sui programmi potenzialmente pericolosi rilevati dall'applicazione, vedere l'Enciclopedia dei Virus all'indirizzo www.viruslist.com. Dopo la scansione, questi programmi possono essere bloccati. Poiché molti di essi sono ampiamente utilizzati dagli utenti, è possibile escluderli dalla scansione.

È ad esempio possibile che si utilizzi frequentemente un programma di amministrazione remota, ovvero un programma di accesso remoto che consente di lavorare da un altro computer. Kaspersky Anti-Virus visualizza l'attività di questo programma come potenzialmente pericolosa e potrebbe bloccarla. Se non si desidera bloccare l'applicazione, è necessario creare una regola di esclusione per l'applicazione in modo che venga rilevata come *not-a-virus:RemoteAdmin.Win32.RAdmin.22* secondo l'Enciclopedia dei Virus.

Le *Regole di esclusione* sono insiemi di condizioni utilizzate da Kaspersky Anti-Virus per verificare se è possibile evitare la scansione di un oggetto.

È possibile escludere dalla scansione determinati formati di file, utilizzare una maschera file o escludere una determinata area, ad esempio una cartella o un programma, processi di programma o oggetti in base alla classificazione del tipo di minaccia nell'Enciclopedia dei Virus.

Il *tipo di minaccia* è lo stato assegnato da Kaspersky Anti-Virus a un oggetto durante la scansione. Lo stato viene assegnato in base alla classificazione dei programmi dannosi o potenzialmente pericolosi elencati nell'Enciclopedia dei Virus di Kaspersky Lab.

Quando si aggiunge un'esclusione, viene creata una regola che può essere utilizzata con diversi componenti dell'applicazione, ad esempio Anti-Virus File (vedere la sezione "Protezione del file system del computer" a pagina [43](#)), Anti-Virus Posta (vedere la sezione "Protezione della posta" a pagina [53](#)), Anti-Virus Web (vedere la sezione "Protezione del traffico Web" a pagina [60](#)) e per l'attività di scansione anti-virus.

➡ Per creare una regola di esclusione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Minacce ed Esclusioni**.
3. Nella sezione **Esclusioni**, cliccare sul bottone **Impostazioni**.
4. Nella finestra visualizzata, nella scheda **Regole di esclusione**, cliccare sul collegamento **Aggiungi**.
5. Nella finestra **Regola di esclusione** visualizzata, modificare le impostazioni delle regole di esclusione.

VEDERE ANCHE:

Maschere di esclusione file consentite [109](#)

Maschere dei tipi di minaccia consentiti [109](#)

MASCHERE DI ESCLUSIONE FILE CONSENTITE

Durante la creazione di elenchi di esclusione file, è possibile utilizzare alcune maschere. Le più comuni sono le seguenti:

1. Maschere senza percorsi file:

- ***.exe** – tutti i file con estensione *exe*;
- ***.ex?** – tutti i file con l'estensione *ex?*, dove *?* può rappresentare qualsiasi carattere singolo;
- **test** – tutti i file con il nome *test*.

2. Maschere con percorsi file assoluti:

- **C:\dir*.*** o **C:\dir*** o **C:\dir** – tutti i file contenuti nella cartella *C:\dir*;
- **C:\dir*.exe** – tutti i file con estensione *exe* contenuti nella cartella *C:\dir*;
- **C:\dir*.ex?** – tutti i file con l'estensione *ex?*, nella cartella *C:\dir*, dove *?* può rappresentare qualsiasi carattere singolo;
- **C:\dir\test** – solo il file *C:\dir\test*.

Se si desidera escludere la scansione dei file in tutte le sottocartelle nidificate della cartella specificata, selezionare la casella ☒ **Includi sottocartelle** durante la creazione di una maschera.

3. Maschere con percorsi file:

- **dir*.*** o **dir*** o **dir** – tutti i file contenuti in tutte le cartelle *dir*;
- **dir\test** – tutti i file *test* contenuti nelle cartelle *dir*;
- **dir*.exe** – tutti i file con estensione *exe* contenuti in tutte le cartelle *dir*;
- **dir*.ex?** – tutti i file con l'estensione *ex?*, contenuti in tutte le cartelle *dir*, dove *?* può rappresentare qualsiasi carattere singolo.

Se si desidera escludere la scansione dei file in tutte le sottocartelle nidificate della cartella specificata, selezionare la casella ☒ **Includi sottocartelle** durante la creazione di una maschera.

Le maschere di esclusione ****** e ***** possono essere utilizzate solo se si specifica il tipo di classificazione della minaccia indicato nell'Enciclopedia dei Virus. In questo caso la minaccia specificata non verrà rilevata in alcun oggetto. L'utilizzo di queste maschere senza specificare il tipo di classificazione in sostanza disabilita il monitoraggio. Durante l'impostazione di un'esclusione, non è consigliabile selezionare un percorso relativo di un disco di rete creato in base a una cartella del file system mediante il comando *subst*, nonché di un disco che rispecchia una cartella di rete. Potrebbe accadere infatti che a risorse diverse venga assegnato lo stesso nome del disco per utenti diversi, con l'inevitabile conseguenza di attivare in modo errato le regole di esclusione.

MASCHERE DEI TIPI DI MINACCIA CONSENTITI

Quando si aggiungono maschere per escludere determinate minacce in base alla relativa classificazione nell'Enciclopedia dei Virus, è possibile specificare le impostazioni seguenti:

- Il nome completo della minaccia come indicato nell'Enciclopedia dei Virus all'indirizzo www.viruslist.com, ad esempio *not-a-virus:RiskWare.RemoteAdmin.RA.311* o *Flooder.Win32.Fuxx*.
- Il nome della minaccia in base alla maschera, ad esempio:
 - **not-a-virus*** - esclude i programmi legali ma potenzialmente pericolosi dalla scansione, oltre ai programmi *joke*;
 - ***Riskware.*** - esclude il *riskware* dalla scansione;
 - ***RemoteAdmin.*** - esclude tutti i programmi di amministrazione remota dalla scansione.

RETE

Nella sezione **Rete** della finestra delle impostazioni dell'applicazione è possibile selezionare le porte monitorate da Kaspersky Anti-Virus e configurare la scansione delle connessioni crittografate:

creare un elenco di porte monitorate;

abilitare/disabilitare la modalità di scansione delle connessioni crittografate utilizzando il protocollo SSL (vedere pagina [111](#));

modificare le impostazioni del server proxy (vedere pagina [113](#)).

VEDERE ANCHE:

Creazione di un elenco delle porte monitorate	110
Scansione delle connessioni crittografate	111
Scansione delle connessioni crittografate in Mozilla Firefox.....	112
Scansione delle connessioni crittografate in Opera.....	113
Impostazioni del server proxy	113

CREAZIONE DI UN ELENCO DELLE PORTE MONITORATE

I componenti della protezione, ad esempio Anti-Virus Posta (vedere la sezione "Protezione della posta" a pagina [53](#)) e Anti-Virus Web (vedere la sezione "Protezione del traffico Web" a pagina [60](#)), monitorano i flussi di dati trasmessi tramite determinati protocolli che attraversano specifiche porte aperte del computer. Anti-Virus Posta, ad esempio, analizza le informazioni trasferite tramite il protocollo SMTP mentre Anti-Virus Web analizza i pacchetti HTTP.

È possibile selezionare una delle due modalità di monitoraggio delle porte:

-  **Tutte le porte di rete;**
-  **Soltanto le porte selezionate.** L'applicazione comprende un elenco delle porte utilizzate per trasmettere la posta elettronica e il traffico HTTP.

➡ *Per aggiungere una porta all'elenco delle porte monitorate:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Rete**.
3. Nella sezione **Porte monitorate** cliccare sul bottone **Seleziona**.
4. Nella finestra **Porte di rete** visualizzata, cliccare sul collegamento **Aggiungi**.
5. Nella finestra **Porta di rete** visualizzata, specificare i dati richiesti.

➡ *Per escludere una porta dall'elenco di porte monitorate:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Rete**.
3. Nella sezione **Porte monitorate** cliccare sul bottone **Seleziona**.
4. Nella finestra **Porte di rete** visualizzata, deselezionare la casella ☒ accanto alla descrizione della porta.

➡ *Per creare l'elenco delle applicazioni per le quali si desidera monitorare tutte le porte, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Rete**.
3. Nella sezione **Porte monitorate** cliccare sul bottone **Seleziona**.
4. Nella finestra **Porte di rete** visualizzata, selezionare la casella ☒ **Controlla tutte le porte per le applicazioni specificate** e cliccare sul collegamento **Aggiungi** nella sezione in basso.
5. Nel menu visualizzato, selezionare un'applicazione. Quando si seleziona la voce **Sfoglia**, viene aperta una finestra nella quale è necessario specificare il percorso di un file eseguibile. Quando si seleziona la voce **Applicazioni**, viene aperto l'elenco di applicazioni attualmente in esecuzione.
6. Nella finestra **Applicazione** visualizzata, specificare la descrizione per l'applicazione selezionata.

SCANSIONE DELLE CONNESSIONI CRITTOGRAFATE

La connessione mediante il protocollo SSL (Secure Sockets Layer) consente di proteggere il canale di scambio dei dati in Internet. Il protocollo SSL è in grado di identificare le parti che scambiano dati tramite certificati elettronici, codificare i dati trasferiti e garantirne l'integrità durante il trasferimento.

Queste funzioni del protocollo vengono utilizzate dai pirati informatici per diffondere programmi dannosi, poiché quasi tutti i programmi anti-virus non esaminano il traffico SSL.

Kaspersky Anti-Virus verifica le connessioni protette utilizzando il certificato di Kaspersky Lab. Tale certificato verrà sempre utilizzato per controllare se la connessione è sicura.

Scansioni successive del traffico tramite il protocollo SSL verranno eseguite utilizzando il certificato di Kaspersky Lab installato. In caso di rilevamento di un certificato non valido durante la connessione al server, ad esempio se il certificato viene sostituito da un intruso, verrà visualizzata una notifica che suggerisce di accettare o rifiutare il certificato o visualizzarne le informazioni. Se l'applicazione funziona in modalità automatica, la connessione che utilizza un certificato non valido verrà interrotta senza notifica.

➡ *Per abilitare la scansione delle connessioni crittografate, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Rete**.
3. Nella finestra visualizzata, selezionare la casella ☒ **Scansione delle connessioni crittografate** e cliccare sul bottone **Installa certificato**.
4. Nella finestra visualizzata, cliccare sul bottone **Installa certificato**. In questo modo viene avviata una procedura guidata che contiene le istruzioni da seguire per installare correttamente il certificato.

L'installazione automatica del certificato è disponibile solo in Microsoft Internet Explorer. Per eseguire la scansione delle connessioni crittografate in Mozilla Firefox e Opera, è necessario installare il certificato di Kaspersky Lab manualmente.

SCANSIONE DELLE CONNESSIONI CRITTOGRAFATE IN MOZILLA FIREFOX

Il browser Mozilla Firefox non utilizza la memoria certificati di Microsoft Windows. Per eseguire la scansione delle connessioni SSL in Mozilla Firefox, è necessario installare il certificato di Kaspersky Lab manualmente.

➡ Per installare il certificato di Kaspersky Lab, eseguire le operazioni seguenti:

1. Selezionare la voce **Tools (Strumenti)** → **Settings (Impostazioni)** nel menu del browser.
2. Nella finestra visualizzata, selezionare la sezione **Additional (Avanzate)**.
3. Nella sezione **Certificates (Certificati)**, selezionare la scheda **Security (Protezione)** e cliccare sul bottone **Viewing certificates (Visualizzazione certificati)**.
4. Nella finestra visualizzata, selezionare la scheda **Certification Centers (Centri certificati)** e cliccare sul bottone **Restore (Ripristina)**.
5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer`
6. Nella finestra visualizzata, selezionare le caselle relative alle azioni da sottoporre a scansione con il certificato installato. Per visualizzare le informazioni relative al certificato, cliccare sul bottone **View (Visualizza)**.

➡ Per installare il certificato di Kaspersky Lab per Mozilla Firefox versione 3.x, eseguire le operazioni seguenti:

1. Selezionare la voce **Tools (Strumenti)** → **Settings (Impostazioni)** nel menu del browser.
2. Nella finestra visualizzata, selezionare la sezione **Additional (Avanzate)**.
3. Nella scheda **Encryption (Crittografia)**, cliccare sul bottone **Viewing certificates (Visualizzazione certificati)**.
4. Nella finestra visualizzata, selezionare la scheda **Certification Centers (Centri certificati)** e cliccare sul bottone **Import (Importa)**.
5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer`
6. Nella finestra visualizzata, selezionare le caselle relative alle azioni da sottoporre a scansione con il certificato installato. Per visualizzare le informazioni relative al certificato, cliccare sul bottone **View (Visualizza)**.

Se nel computer è in esecuzione Microsoft Windows Vista, il percorso del file di certificato di Kaspersky Lab sarà il seguente: `%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer`.

SCANSIONE DELLE CONNESSIONI CRITTOGRAFATE IN OPERA

Il browser Opera non utilizza la memoria certificati di Microsoft Windows. Per eseguire la scansione delle connessioni SSL in Opera, è necessario installare il certificato di Kaspersky Lab manualmente.

➡ Per installare il certificato di Kaspersky Lab, eseguire le operazioni seguenti:

1. Selezionare la voce **Tools (Strumenti)** → **Settings (Impostazioni)** nel menu del browser.
2. Nella finestra visualizzata, selezionare la sezione **Additional (Avanzate)**.
3. Nella parte sinistra della finestra, selezionare la scheda **Security (Protezione)** e cliccare sul bottone **Manage Certificates (Gestisci certificati)**.
4. Nella finestra visualizzata, selezionare la scheda **Vendors (Fornitori)** e cliccare sul bottone **Import (Importa)**.
5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
6. Nella finestra visualizzata, cliccare sul bottone **Install (Installa)**. Il certificato di Kaspersky Lab verrà installato. Per visualizzare le informazioni sul certificato e selezionare le azioni per le quali verrà utilizzato il certificato, selezionare il certificato nell'elenco e cliccare sul bottone **View (Visualizza)**.

➡ Per installare il certificato di Kaspersky Lab per Opera versione 9.x, eseguire le operazioni seguenti:

1. Selezionare la voce **Strumenti** → **Impostazioni** nel menu del browser.
2. Nella finestra visualizzata, selezionare la sezione **Additional (Avanzate)**.
3. Nella parte sinistra della finestra, selezionare la scheda **Security (Protezione)** e cliccare sul bottone **Manage Certificates (Gestisci certificati)**.
4. Nella finestra visualizzata, selezionare la scheda **Certification Centers (Centri certificati)** e cliccare sul bottone **Import (Importa)**.
5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
6. Nella finestra visualizzata, cliccare sul bottone **Install (Installa)**. Il certificato di Kaspersky Lab verrà installato.

Se nel computer è in esecuzione Microsoft Windows Vista, il percorso del file di certificato di Kaspersky Lab sarà il seguente: `%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`

IMPOSTAZIONI DEL SERVER PROXY

Se la connessione a Internet del computer viene stabilita tramite un server proxy, potrebbe essere necessario modificarne le impostazioni di connessione. Kaspersky Anti-Virus utilizza tali impostazioni per determinati componenti di protezione, nonché per l'aggiornamento dei moduli di applicazione e dei database.

Se la rete include un server proxy che utilizza una porta non standard, aggiungere il numero di porta all'elenco di porte monitorate.

➡ *Per configurare il server proxy, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Rete**.
3. Nella sezione **Server proxy**, cliccare sul bottone **Impostazioni del server proxy**.
4. Nella finestra **Impostazioni del server proxy** visualizzata, modificare le impostazioni del server proxy.

NOTIFICHE

Durante il funzionamento di Kaspersky Anti-Virus, si verificano diversi tipi di eventi di carattere informativo o contenenti dati importanti. Un evento può ad esempio informare l'utente del completamento con esito positivo di un aggiornamento dell'applicazione o registrare un errore nel funzionamento di un determinato componente che deve essere eliminato immediatamente.

Per essere aggiornati sugli eventi che si verificano durante il funzionamento di Kaspersky Anti-Virus, utilizzare il servizio di notifica.

Per impostazione predefinita, l'utente riceve notifica degli eventi mediante messaggi a comparsa caratterizzati da un segnale audio.

Le notifiche possono essere inviate in uno dei seguenti modi:

- messaggi a comparsa che vengono visualizzati sopra l'icona dell'applicazione nell'area di notifica;
- messaggi audio;
- messaggi di posta elettronica.

➡ *Per disabilitare l'invio di notifiche, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Notifiche**.
3. Deselezionare la casella ☒ **Attiva le notifiche degli eventi**.

Anche se l'invio di notifiche è disabilitato, le informazioni sugli eventi che si verificano durante il funzionamento di Kaspersky Anti-Virus verranno registrate nel rapporto sul funzionamento dell'applicazione.

➡ *Per selezionare il metodo di invio delle notifiche, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la scheda **Notifiche** e cliccare sul bottone **Impostazioni**.
3. Nella finestra **Notifiche** visualizzata, selezionare il metodo di invio delle notifiche.

VEDERE ANCHE:

Disabilitazione delle notifiche con segnali acustici	115
Invio di notifiche via posta elettronica	115

DISABILITAZIONE DELLE NOTIFICHE CON SEGNALI ACUSTICI

Per impostazione predefinita, tutte le notifiche sono accompagnate da un segnale acustico per il quale viene utilizzata la combinazione di suoni Microsoft Windows. La casella ☒ **Usa i suoni standard di Microsoft Windows** consente di scegliere una combinazione diversa. Se la casella è deselezionata, verrà utilizzata la combinazione di suoni usata nelle versioni precedenti dell'applicazione.

➡ *Per disabilitare le notifiche con segnali acustici, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Notifiche**.
3. Deselezionare la casella ☒ **Attiva le notifiche acustiche**.

INVIO DI NOTIFICHE VIA POSTA ELETTRONICA

Se le notifiche devono essere inviate tramite posta elettronica, modificare le impostazioni di invio.

➡ *Per modificare le impostazioni della posta elettronica per l'invio di notifiche, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Notifiche**.
3. Selezionare la casella ☒ **Attiva le notifiche via e-mail** e cliccare sul bottone **Impostazioni e-mail**.
4. Nella finestra **Impostazioni delle notifiche via e-mail** visualizzata, specificare le impostazioni di invio.

RAPPORTI E BACKUP

In questa sezione sono contenute le impostazioni che controllano il funzionamento dei file di dati di Kaspersky Anti-Virus.

I *file di dati dell'applicazione* sono oggetti messi in quarantena da Kaspersky Anti-Virus o spostati nella cartella Backup, nonché file contenenti rapporti sul funzionamento dei componenti dell'applicazione.

In questa sezione, è possibile:

- modificare le impostazioni per la creazione (vedere pagina [116](#)) e l'archiviazione dei rapporti (vedere pagina [117](#));
- modificare le impostazioni per la quarantena e il backup (vedere pagina [118](#)).

VEDERE ANCHE:

Registrazione degli eventi nei rapporti.....	116
Cancellazione del contenuto dei rapporti dell'applicazione	116
Archiviazione di rapporti	117
Quarantena per oggetti potenzialmente infetti.....	117
Copie di backup degli oggetti pericolosi	118
Azioni con gli oggetti in quarantena.....	118
Archiviazione degli oggetti della quarantena e del backup	118
Rapporti.....	128

REGISTRAZIONE DEGLI EVENTI NEI RAPPORTI

È possibile aggiungere al rapporto informazioni su eventi non critici, eventi di registro e relativi al file system. Per impostazione predefinita, tali eventi non vengono registrati nei rapporti.

➡ *Per aggiungere al rapporto informazioni su eventi non critici, eventi di registro e relativi al file system:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Rapporti e Backup**.
3. Nella sezione **Rapporti**, selezionare la casella ☒ desiderata.

CANCELLAZIONE DEL CONTENUTO DEI RAPPORTI DELL'APPLICAZIONE

Nei rapporti sono contenute informazioni sul funzionamento di Kaspersky Anti-Virus. Tali informazioni possono essere cancellate.

➡ *Per cancellare i rapporti, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Rapporti e Backup**.
3. Nella sezione **Rapporti**, cliccare sul bottone **Cancella**.
4. Nella finestra **Eliminazione dei rapporti** visualizzata, selezionare le casella relative alle categorie di rapporti che si desidera cancellare.

ARCHIVIAZIONE DI RAPPORTI

È possibile determinare la durata massima di archiviazione dei rapporti sugli eventi (casella ☒ **Mantieni i rapporti per non più di**). Per impostazione predefinita, tale valore corrisponde a 30 giorni. Una volta trascorso questo periodo, gli oggetti vengono eliminati. È possibile modificare la durata massima di archiviazione o persino eliminare eventuali limiti imposti su tale valore. È inoltre possibile specificare la dimensione massima del file del rapporto (casella ☒ **Dimensione massima del file**). Per impostazione predefinita, la dimensione massima è di 1024 MB. Una volta raggiunte le dimensioni massime, il contenuto del file verrà sovrascritto con le nuove voci. È possibile annullare eventuali limiti impostati sulla dimensione del rapporto o immettere un altro valore.

➡ Per configurare le impostazioni dell'archiviazione dei rapporti, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Rapporti e Backup**.
3. Nella finestra visualizzata, sezione **Rapporti**, selezionare le caselle ☒ desiderate e modificare la massima dimensione e durata di archiviazione del rapporto in base alle esigenze.

QUARANTENA PER OGGETTI POTENZIALMENTE INFETTI

Quarantena è uno speciale repository in cui vengono memorizzati gli oggetti che potrebbero essere stati infettati da virus.

Gli oggetti potenzialmente infetti sono oggetti sospettati di essere stati infettati da virus o relative varianti.

Un oggetto potenzialmente infetto può essere individuato e messo in quarantena da Anti-Virus File, Anti-Virus Posta, Difesa Proattiva o durante una scansione anti-virus.

Gli oggetti vengono messi in quarantena in seguito al funzionamento di Anti-Virus File e Anti-Virus Posta, nonché nel corso di una scansione anti-virus, se:

- *Il codice dell'oggetto analizzato ricorda quello di una minaccia nota ma è in parte modificato.*

I database di Kaspersky Anti-Virus contengono le informazioni aggiornate sulle minacce individuate dagli specialisti di Kaspersky Lab. Se un programma dannoso viene modificato e le modifiche non sono state ancora inserite nei database, Kaspersky Anti-Virus classifica l'oggetto infetto con il programma dannoso modificato come oggetto potenzialmente infetto e indica con esattezza la minaccia alla quale somiglia questa infezione.

- *La struttura del codice dell'oggetto rilevato ricorda un programma dannoso; tuttavia nei database dell'applicazione non è stato registrato nulla di simile.*

È abbastanza probabile che si tratti di un nuovo tipo di minaccia, pertanto Kaspersky Anti-Virus classifica l'oggetto come oggetto potenzialmente infetto.

I file vengono identificati come potenzialmente infetti da un virus dall'*analizzatore euristico di codice*. Questo meccanismo è estremamente efficace e determina falsi positivi molto raramente.

Come per Difesa Proattiva, il componente mette un oggetto in quarantena se, come risultato dell'analisi del comportamento, la sequenza di azioni dell'oggetto desta sospetti.

Quando si mette un oggetto in Quarantena, l'oggetto viene spostato e non copiato. Esso viene eliminato dal disco o dalla posta elettronica e salvato nella cartella Quarantena. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

È possibile che al termine dell'aggiornamento del database Kaspersky Anti-Virus riesca a identificare la minaccia in modo inequivocabile e neutralizzarla. Per questo motivo, l'applicazione esamina gli oggetti in quarantena dopo ogni aggiornamento (vedere pagina [91](#)).

COPIE DI BACKUP DEGLI OGGETTI PERICOLOSI

In alcuni casi non è possibile mantenere l'integrità degli oggetti durante la disinfezione. Se il file disinfettato contiene informazioni importanti, e dopo la disinfezione diventa in parte o del tutto inaccessibile, è possibile provare a ripristinare l'oggetto originale dalla copia di backup.

La *copia di backup* è una copia dell'oggetto pericoloso originale creata quando l'oggetto è stato disinfettato o eliminato per la prima volta e salvata sotto forma di backup.

Backup è uno speciale repository che contiene copie di backup degli oggetti pericolosi dopo l'elaborazione o l'eliminazione. La principale funzione dell'archivio di backup è la possibilità di ripristinare in qualsiasi momento l'oggetto originale. I file del backup vengono salvati in un formato speciale e non costituiscono un pericolo.

AZIONI CON GLI OGGETTI IN QUARANTENA

È possibile eseguire le azioni seguenti sugli oggetti in quarantena:

- mettere in quarantena i file sospettati di essere infetti;
- esaminare e disinfettare tutti gli oggetti potenzialmente infetti che sono in quarantena utilizzando i database di Kaspersky Anti-Virus correnti;
- ripristinare i file nelle cartelle da cui sono stati spostati per essere messi in quarantena oppure nelle cartelle selezionate dall'utente;
- eliminare tutti gli oggetti in quarantena oppure un gruppo di oggetti selezionati.
- inviare gli oggetti in quarantena a Kaspersky Lab per l'analisi.

➡ *Per eseguire azioni sugli oggetti in quarantena:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Quarantena**.
2. Eseguire le azioni richieste nella scheda **Minacce rilevate** della finestra che viene visualizzata.

ARCHIVIAZIONE DEGLI OGGETTI DELLA QUARANTENA E DEL BACKUP

È possibile modificare le impostazioni seguenti per la quarantena e il backup:

- Determinare il tempo di archiviazione massimo per gli oggetti in quarantena e per le copie degli oggetti nel backup (casella ☒ **Mantieni gli oggetti per non più di**). Per impostazione predefinita, la durata di archiviazione degli oggetti è di 30 giorni. Una volta trascorso questo periodo, gli oggetti vengono eliminati. È possibile modificare il termine archiviazione massima o rimuovere del tutto questa restrizione.
- Specificare la dimensione massima dell'area di archiviazione dei dati (casella ☒ **Dimensione massima**). Per impostazione predefinita, la dimensione massima è di 100 MB. È possibile annullare il limite delle dimensioni del rapporto o impostare un altro valore.

➡ *Per configurare le impostazioni della quarantena e del backup:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Rapporti e Backup**.
3. Nella sezione **Quarantena e Backup**, selezionare le caselle desiderate e immettere la dimensione massima dell'area di archiviazione dei dati in base alle esigenze.

FEEDBACK

In tutto il mondo appaiono quotidianamente numerose nuove minacce. Per facilitare la raccolta di statistiche sui nuovi tipi di minaccia, sulle relative origini, nonché sui metodi da utilizzare per eliminarle, Kaspersky Lab consiglia l'utilizzo del servizio *Kaspersky Security Network*.

L'utilizzo di Kaspersky Security Network richiede l'invio di determinate informazioni a Kaspersky Lab, tra le quali figurano le seguenti:

- Identificatore univoco assegnato al computer dall'applicazione di Kaspersky Lab. Questo identificatore caratterizza le impostazioni hardware del computer e non contiene informazioni riservate.
- Informazioni sulle minacce identificate dai componenti dell'applicazione. La struttura e il contenuto delle informazioni dipendono dal tipo di minaccia rilevata.
- Informazioni sul sistema operativo: versione del sistema operativo, service pack installati, servizi e driver scaricati, versioni del browser e del client di posta elettronica, estensioni del browser, numero di versione dell'applicazione Kaspersky Lab installata.

➡ Per abilitare l'invio di statistiche in Kaspersky Security Network, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Feedback**.
3. Selezionare la casella ☒ **Accetto di partecipare al programma Kaspersky Security Network**.

ASPETTO DELL'APPLICAZIONE

È possibile modificare l'aspetto di Kaspersky Anti-Virus creando e utilizzando diversi schemi grafici e cromatici. È inoltre possibile configurare l'uso di vari elementi attivi dell'interfaccia, come l'icona dell'applicazione nell'area di notifica della barra delle applicazioni di Microsoft Windows o i messaggi a comparsa.

VEDERE ANCHE:

Elementi attivi dell'interfaccia.....	119
Interfaccia dell'applicazione.....	120

ELEMENTI ATTIVI DELL'INTERFACCIA

Per configurare le impostazioni degli elementi attivi dell'interfaccia, quali l'icona di Kaspersky Anti-Virus nell'area di notifica e i messaggi a comparsa, è possibile utilizzare le funzioni seguenti dell'applicazione:

Anima l'icona sulla barra delle applicazioni durante l'esecuzione delle attività.

L'icona dell'applicazione nell'area di notifica cambia in base all'operazione eseguita dall'applicazione. Se, ad esempio, è in corso la scansione di uno script, compare il disegno di uno script sul fondo dell'icona, mentre se è in corso la scansione di un messaggio di posta elettronica, viene visualizzata l'immagine di una lettera. L'icona di Kaspersky Anti-Virus è animata. In questo caso, verrà indicato solo lo stato di protezione del computer: se la protezione è abilitata, l'icona è colorata, se invece è sospesa o disabilitata, l'icona è grigia.

Attiva le finestre semi-trasparenti.

Tutte le operazioni dell'applicazione che richiedono un'attenzione immediata o una decisione vengono presentate come messaggi a comparsa visualizzati al di sopra dell'icona dell'applicazione nell'area di notifica. Le finestre del messaggio sono trasparenti in modo da non interferire con il lavoro. La trasparenza viene persa quando si posiziona il cursore sulla finestra del messaggio.

Attiva le notifiche delle notizie.

Per impostazione predefinita, quando vengono ricevute notizie, l'area di notifica visualizza un'icona speciale che, se selezionata mediante clic, raffigura una finestra contenente la notizia.

Mostra "Protected by Kaspersky Lab" nella schermata di accesso a Microsoft Windows.

Per impostazione predefinita, questo indicatore viene visualizzato nell'angolo superiore destro della schermata all'avvio di Kaspersky Anti-Virus e informa l'utente che il computer è protetto da qualsiasi tipo di minaccia.

Se l'applicazione viene installata in un computer che utilizza Microsoft Windows Vista, questa opzione non è disponibile.

➡ Per configurare gli elementi attivi dell'interfaccia, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Aspetto**.
3. Nel blocco **Icona nell'area di notifica della barra delle applicazioni**, selezionare o deselezionare le caselle ☒ appropriate.

INTERFACCIA DELL'APPLICAZIONE

Tutti i colori, i caratteri, le icone e gli elementi di testo utilizzati nell'interfaccia di Kaspersky Anti-Virus possono essere modificati. È possibile creare interfacce personalizzate per l'applicazione o localizzarle in un'altra lingua.

➡ Per utilizzare un'altra interfaccia per l'applicazione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Aspetto**.
3. Selezionare la casella ☒ **Usa un'interfaccia alternativa** nella sezione **Interfacce** per attivare un'interfaccia. Specificare la cartella con le impostazioni dell'interfaccia nel campo di immissione. Per salvare la cartella, cliccare sul bottone **Sfoglia**.

UTILIZZO DEI PROFILI DI KASPERSKY ANTI-VIRUS

L'utilizzo di alcune applicazioni in modalità schermo intero, ad esempio i giochi, potrebbe rendere necessaria la disabilitazione di determinate funzioni di Kaspersky Anti-Virus, come il servizio di notifica. Inoltre, poiché tali applicazioni richiedono una notevole quantità di risorse del sistema, l'esecuzione di alcune attività di Kaspersky Anti-Virus potrebbe rallentarne le prestazioni.

Per evitare di dover disabilitare manualmente le notifiche e sospendere le attività a ogni avvio di applicazioni a schermo intero, Kaspersky Anti-Virus include la possibilità di modificare temporaneamente le impostazioni mediante il profilo di gioco. Tale profilo consente di modificare simultaneamente le impostazioni di tutti i componenti durante il passaggio alla modalità a schermo intero e di ripristinare le modifiche apportate una volta usciti da tale modalità.

Nel passaggio alla modalità a schermo intero, le notifiche degli eventi verranno disabilitate automaticamente. È inoltre possibile specificare le impostazioni seguenti:

- ☒ **Scegli l'azione automaticamente.** Se questa impostazione è selezionata, la selezione automatica dell'azione verrà applicata di conseguenza a tutti i componenti, anche se l'opzione  **Chiedi di scegliere un'azione** è selezionata nelle rispettive impostazioni. Pertanto l'azione da eseguire sulle minacce rilevate verrà selezionata automaticamente e non verrà richiesto all'utente di farlo.
- ☒ **Non eseguire gli aggiornamenti** e ☒ **Non eseguire le attività di scansione pianificate.** È consigliabile utilizzare queste impostazioni per evitare di rallentare le prestazioni delle applicazioni a schermo intero.

➡ *Per abilitare il profilo di gioco, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Profilo Gioco**.
3. Selezionare la casella ☒ **Abilita Profilo Gioco** e specificare le impostazioni richieste.

FUNZIONI AVANZATE

Garantire la protezione del computer è un'attività complessa che richiede una conoscenza approfondita delle funzioni del sistema operativo e dei metodi che minacciano i punti deboli. D'altro canto, la grande quantità e varietà di informazioni sulla protezione dei sistemi ne complica l'analisi e l'elaborazione.

Per facilitare la risoluzione di attività specifiche mirate a garantire la protezione del computer, nel pacchetto di Kaspersky Anti-Virus è stato incluso un insieme di procedure guidate e di strumenti.

- Lo strumento Tastiera Virtuale (vedere pagina [122](#)) previene l'intercettazione dei dati immessi tramite tastiera.
- La Creazione guidata del Disco di Ripristino (vedere pagina [123](#)) consente di ripristinare l'operatività del sistema dopo l'attacco di un virus o se i file di sistema del sistema operativo sono danneggiati e non è possibile riavviarlo nello stato precedente.
- La Configurazione guidata del browser (vedere pagina [125](#)) consente di eseguire l'analisi e la valutazione delle impostazioni di Microsoft Internet Explorer, innanzitutto rispetto alla protezione.
- Il Ripristino guidato del sistema (vedere pagina [126](#)) elimina le tracce della presenza di oggetti malware nel sistema.
- La Pulizia guidata dei dati riservati (vedere pagina [127](#)) cerca ed elimina le tracce delle attività dell'utente nel sistema.

IN QUESTA SEZIONE:

Tastiera Virtuale	122
Disco di Ripristino	123
Configurazione del browser	125
Ripristino dopo un'infezione	126
Pulizia guidata dei dati riservati	127

TASTIERA VIRTUALE

L'utilizzo del computer implica spesso situazioni in cui è necessario immettere i propri dati personali o il nome utente e la password, ad esempio quando si effettua una registrazione ai siti Web, quando si utilizzano negozi online e così via.

In tal caso, esiste il rischio che le informazioni personali siano intercettate tramite intercettori di eventi tastiera o keylogger, ovvero programmi che memorizzano le sequenze di tasti.

Lo strumento tastiera virtuale previene l'intercettazione dei dati immessi tramite tastiera.

La tastiera virtuale non può proteggere i dati riservati se il sito che richiede l'immissione di tali dati è stato hackerato; in tal caso, infatti, le informazioni verranno ottenute direttamente dagli intrusi.

Molte delle applicazioni classificate come spyware svolgono la funzione di creare screenshot che vengono quindi trasferiti a un intruso che li analizzerà per trafugare i dati personali dell'utente. La tastiera virtuale previene l'intercettazione dei dati immessi tramite tastiera.

Ma solo quando si lavora con i browser Microsoft Internet Explorer e Mozilla Firefox.

► *Per utilizzare la tastiera virtuale:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la sezione **Protezione+** nella parte sinistra della finestra e cliccare sul bottone **Tastiera Virtuale**.
3. Immettere i dati richiesti premendo i tasti della tastiera virtuale. Verificare che i dati siano immessi nel campo corretto. Se si premono i tasti funzione (**Maiusc**, **Alt**, **Ctrl**) della tastiera virtuale, viene impostata la modalità di immissione specificata, ad esempio premendo **Maiusc** tutti i simboli verranno immessi in maiuscolo. Per uscire dalla modalità selezionata, premere nuovamente lo stesso tasto funzione.

È possibile alternare le lingue della tastiera virtuale facendo clic con il pulsante destro del mouse sul pulsante **Shift** tenendo contemporaneamente premuto **Ctrl** oppure facendo clic con il pulsante destro del mouse sul pulsante **Alt** di sinistra tenendo contemporaneamente premuto il tasto **Ctrl**, in base alla configurazione corrente.

DISCO DI RIPRISTINO

Kaspersky Anti-Virus comprende un servizio che consente di creare un Disco di Ripristino.

Disco di Ripristino è stato progettato per eseguire la scansione dei computer compatibili con le piattaforme x86 e per disinfettarli. È consigliabile utilizzarlo quando il livello di infezione è tale da reputare impossibile la disinfezione tramite applicazioni anti-virus o utilità di rimozione di malware, ad esempio Kaspersky AVPTool, del sistema operativo. In questo caso, è possibile ottenere un livello di efficacia della disinfezione superiore, in quanto i programmi malware non ottengono il controllo quando viene caricato il sistema operativo.

Disco di Ripristino è un file con estensione iso basato sulla piattaforma Linux che include gli elementi seguenti:

- file Linux di sistema e di configurazione;
- una serie di utilità diagnostiche per il sistema operativo;
- una serie di strumenti aggiuntivi (gestione file e così via);
- file di Disco di Ripristino Kaspersky;
- file contenenti database anti-virus.

Un computer con il sistema operativo danneggiato viene avviato da un dispositivo CD/DVD-ROM. A tale scopo, è necessario che il computer sia dotato di un dispositivo appropriato.

► *Per creare un Disco di Ripristino, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la sezione **Protezione+** nella parte sinistra della finestra.
3. Cliccare sul bottone **Creazione di un Disco di Ripristino** per eseguire la creazione guidata del disco.
4. Seguire le istruzioni della procedura guidata.
5. Utilizzando il file fornito con la procedura guidata, creare un CD/DVD di avvio. A tale scopo, è possibile utilizzare un'applicazione di masterizzazione di CD/DVD, come Nero.

VEDERE ANCHE:

Creazione del Disco di Ripristino.....	124
Avvio del computer attraverso il Disco di Ripristino.....	124

CREAZIONE DEL DISCO DI RIPRISTINO

La creazione del Disco di Ripristino comporta la creazione di un'immagine del disco (file ISO) con database e file di configurazione anti-virus aggiornati.

L'immagine del disco di origine da utilizzare come base per la creazione del nuovo file può essere scaricata dal server Kaspersky Lab o copiata da un'origine locale.

Il file di immagine creato mediante la procedura guidata verrà salvato nella cartella "*Documents and Settings\All Users\Dati applicazioni\Kaspersky Lab\AVP9\Data\Rdisk*", o "*ProgramData\Kaspersky Lab\AVP9\Data\Rdisk*" per Microsoft Vista e verrà denominato *rescuecd.iso*. Se la procedura guidata rileva un file ISO creato in precedenza nella cartella specificata, è possibile utilizzarlo come immagine del disco originale selezionando la casella ☒ **Usa file ISO esistente** e andare al Passaggio 3. Aggiornamento del file di immagine. Se la procedura guidata non rileva alcun file di immagine, questa casella non sarà disponibile.

Disco di Ripristino viene creato mediante una procedura guidata costituita da una serie di caselle (passaggi) visualizzabili mediante i pulsanti **Indietro** e **Avanti**. Per terminare la procedura, cliccare sul bottone **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il bottone **Annulla**.

VEDERE ANCHE:

Disco di Ripristino.....	123
Avvio del computer attraverso il Disco di Ripristino.....	124

AVVIO DEL COMPUTER ATTRAVERSO IL DISCO DI RIPRISTINO

Se non è possibile eseguire l'avvio del sistema operativo a causa dell'attacco di un virus, utilizzare il Disco di Ripristino.

Per caricare il sistema operativo, sarà necessario il file di immagine del disco di avvio (con estensione iso). È possibile scaricare un file ISO dal server Kaspersky Lab o aggiornare quello esistente.

Di seguito viene illustrato in modo dettagliato il funzionamento del Disco di Ripristino. Durante il caricamento del disco, vengono eseguite le operazioni seguenti:

1. Rilevamento automatico dell'hardware del computer.
2. Ricerca dei file system nei dischi rigidi. Ai file system rilevati verranno assegnati nomi che iniziano con "C".

È possibile che ai dischi rigidi e ai dispositivi rimovibili vengano assegnati nomi che non corrispondono a quelli assegnati dal sistema operativo.

Se il sistema operativo del computer caricato è in modalità di sospensione o se il relativo file system presenta lo stato *infetto* a causa di una chiusura non corretta, l'utente potrà scegliere se installare il file system o riavviare il computer.

L'installazione del file system potrebbe comportarne il danneggiamento.

3. Ricerca del file swap di Microsoft Windows *pagefile.sys*. Se tale file è assente, il volume della memoria virtuale sarà limitato dalla dimensione della RAM.
4. Selezione della lingua di localizzazione. Se la selezione non viene effettuata dopo un determinato intervallo di tempo, per impostazione predefinita verrà impostata la lingua inglese.
5. Ricerca (creazione) nelle cartelle di database anti-virus, rapporti, memoria di quarantena e file aggiuntivi. Per impostazione predefinita, verranno utilizzate le cartelle delle applicazioni di Kaspersky Lab installate nel computer infetto (*ProgramData/Kaspersky Lab/AVP8* - per Microsoft Windows Vista, *Documents and Settings/All Users/Dati applicazioni/Kaspersky Lab/AVP8* - per le versioni precedenti di Microsoft Windows). Se non è possibile individuare tali cartelle, verrà effettuato il tentativo di crearle. Se non è possibile trovare le cartelle né crearle, la cartella *kl.files* verrà creata in un disco di sistema.
6. Tentativo di configurazione delle connessioni di rete in base ai dati rilevati nei system file del computer di cui è in corso il caricamento.
7. Caricamento del sottosistema grafico e avvio del Disco di Ripristino Kaspersky.

Nella modalità di ripristino del sistema sono disponibili solo le attività di scansione anti-virus e di aggiornamento dei database da un'origine locale, nonché il rollback degli aggiornamenti e la visualizzazione delle statistiche.

► Per caricare il sistema operativo di un computer infetto, eseguire le operazioni seguenti:

1. Nelle impostazioni del BIOS abilitare l'avvio dal CD/DVD-ROM. Per informazioni dettagliate, fare riferimento alla documentazione relativa alla scheda madre installata nel computer.
2. Inserire il CD/DVD con l'immagine del Disco di Ripristino nell'unità CD/DVD di un computer infetto.
3. Riavviare il computer.

Le operazioni di avvio successive verranno eseguite in base all'algoritmo descritto prima. Per ulteriori dettagli sulle funzionalità del Disco di Ripristino, fare riferimento alla Guida del Disco di Ripristino Kaspersky.

VEDERE ANCHE:

Disco di Ripristino.....	123
Creazione del Disco di Ripristino.....	124

CONFIGURAZIONE DEL BROWSER

La Configurazione guidata del browser analizza le impostazioni di Microsoft Internet Explorer valutandole innanzitutto dal punto di vista della protezione. È possibile, infatti, che alcune impostazioni selezionate dall'utente o predefinite possano determinare problemi di protezione.

La procedura guidata verifica se sono stati installati gli ultimi aggiornamenti software del browser e se le relative impostazioni contengono vulnerabilità potenziali utilizzabili dagli intrusi per causare danni al computer. Esempi di oggetti analizzati:

- **La cache di Microsoft Internet Explorer.** La cache contiene dati riservati da cui è possibile ottenere anche una cronologia dei siti Web visitati dall'utente. Alcuni oggetti malware esaminano la cache durante la scansione del disco e gli intrusi possono ottenere l'indirizzo di posta elettronica dell'utente. Si consiglia di cancellare il contenuto della cache ogni volta che si chiude il browser.
- **Visualizzazione delle estensioni dei file di formato conosciuto.** Un'opzione di Esplora risorse consente di nascondere le estensioni dei file. Alcuni oggetti malware utilizzano l'estensione doppia e in tal caso l'utente può vedere solo una parte del nome file senza l'estensione reale. Questo schema viene utilizzato spesso dagli intrusi. Si consiglia di abilitare la visualizzazione delle estensioni per i file di formato conosciuto.
- **L'elenco di siti attendibili.** Gli oggetti malware possono aggiungere a questo elenco collegamenti a diversi siti dell'intruso.

Chudere tutte le finestre di Microsoft Internet Explorer prima di avviare la diagnostica.

Una volta completata la revisione, la procedura guidata analizza le informazioni per valutare se sono presenti problemi di protezione del sistema che richiedono attenzione immediata. Compila quindi un elenco di azioni da eseguire per eliminare i problemi. Tali azioni vengono raggruppate in categorie in base alla gravità dei problemi rilevati.

Inoltre, una volta completata la procedura guidata, viene generato un rapporto che può essere inviato a Kaspersky Lab per l'analisi.

Tenere presente che alcune impostazioni possono causare problemi con la visualizzazione di determinati siti (ad esempio se utilizzano controlli ActiveX). Questo problema può essere risolto aggiungendo tali siti all'area attendibile.

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Indietro** e **Avanti**. Per chiudere la procedura guidata al completamento, utilizzare il bottone **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il bottone **Annulla**.

► Per avviare la procedura guidata:

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la sezione **Protezione+** nella parte sinistra della finestra e cliccare sul bottone **Ottimizzazione delle impostazioni del browser Internet**.

RIPRISTINO DOPO UN'INFEZIONE

Il Ripristino guidato del sistema elimina le tracce di azioni di oggetti malware nel sistema. Gli esperti di Kaspersky Lab consigliano di eseguire la procedura guidata dopo aver disinfettato il computer per verificare che tutte le minacce e i danni causati dall'infezione siano stati risolti. Se si sospetta che il computer sia infetto, è possibile anche utilizzare la procedura guidata.

La procedura guidata verifica se sono state apportate modifiche al sistema, ad esempio: il blocco dell'accesso alla rete, la modifica delle estensioni file di formato noto o il blocco della barra degli strumenti. Tali danni possono essere causati dalle azioni dei programmi dannosi, da problemi del sistema e da un funzionamento errato delle applicazioni di ottimizzazione del sistema.

Una volta completata la revisione, la procedura guidata analizza le informazioni raccolte per verificare la presenza di danni del sistema che richiedono attenzione immediata. In base alla revisione, viene generato un elenco di azioni necessarie per eliminare i problemi. Tali azioni vengono raggruppate in categorie in base alla gravità dei problemi rilevati.

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Indietro** e **Avanti**. Per chiudere la procedura guidata al completamento, utilizzare il bottone **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il bottone **Annulla**.

► Per avviare la procedura guidata:

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la sezione **Protezione+** nella parte sinistra della finestra e cliccare sul bottone **Correzione delle impostazioni di Microsoft Windows**.

PULIZIA GUIDATA DEI DATI RISERVATI

Gran parte delle azioni dell'utente del computer viene registrata nel sistema. In questo caso vengono salvati i dati seguenti:

- Cronologie contenenti informazioni:
 - sui siti Web visitati;
 - sugli avvii di un'applicazione;
 - sulle richieste di ricerca;
 - sull'apertura o il salvataggio di file in applicazioni diverse.
- Record del log di sistema di Microsoft Windows.
- File temporanei e così via.

Tutte queste fonti di informazioni sulle attività dell'utente possono contenere dati riservati, incluse le password, e possono diventare disponibili per gli intrusi che le analizzeranno. L'utente spesso non dispone di sufficienti conoscenze per evitare il furto di informazioni con questo metodo.

Kaspersky Anti-Virus include the **Pulizia guidata dei dati riservati**. Questa procedura guidata ricerca le tracce di attività dell'utente nel sistema e le impostazioni del sistema operativo che contribuiscono alla memorizzazione dei dati sulle attività dell'utente.

La memorizzazione delle informazioni sull'attività dell'utente nel sistema è eseguita regolarmente. Viene registrato l'avvio di ogni file o l'apertura di qualsiasi documento. Il log di sistema di Microsoft Windows registra molti eventi che si verificano nel sistema. Per questo motivo, un'esecuzione ripetuta di **Pulizia guidata dei dati riservati** può rilevare tracce di attività non pulite durante la precedente esecuzione della procedura guidata. Alcuni file, ad esempio il file log di Microsoft Windows, possono essere utilizzati nel sistema mentre la procedura guidata cerca di eliminarli. Per eliminare tali file, la procedura guidata suggerisce di riavviare il sistema. Tuttavia, durante il riavvio tali file potrebbero essere ricreati e rilevati nuovamente come tracce di attività.

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Indietro** e **Avanti**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

➡ *Per avviare la procedura guidata:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la sezione **Protezione+** nella parte sinistra della finestra e cliccare sul pulsante **Eliminazione della cronologia delle attività**.

RAPPORTI

Il funzionamento di ogni componente di Kaspersky Anti-Virus e le prestazioni di ogni scansione anti-virus e attività di aggiornamento vengono registrate in un rapporto.

I rapporti consentono di eseguire le operazioni seguenti:

- selezionare il componente o l'attività (vedere pagina [128](#)) per la quale si desidera visualizzare il rapporto sull'evento;
- gestire il raggruppamento dei dati (vedere pagina [129](#)) e la visualizzazione dei dati sullo schermo (vedere pagina [130](#));
- creare una pianificazione (vedere pagina [129](#)) in base alla quale Kaspersky Anti-Virus notificherà all'utente quando il rapporto è pronto;
- selezionare i tipi di evento (vedere pagina [130](#)) per i quali si desidera creare un rapporto;
- selezionare la modalità di visualizzazione delle informazioni statistiche sullo schermo, ovvero grafica o in formato tabella (vedere pagina [132](#));
- salvare un rapporto come file (vedere pagina [132](#));
- specificare condizioni di filtraggio complesso (vedere pagina [133](#));
- configurare la ricerca degli eventi (vedere pagina [134](#)) verificatisi nel sistema ed elaborati dall'applicazione.

IN QUESTA SEZIONE:

Selezione di un componente o di un'attività per creare un rapporto	128
Gestione del raggruppamento delle informazioni nel rapporto	129
Notifica sul completamento del rapporto	129
Selezione dei tipi di evento	130
Visualizzazione dei dati sullo schermo	130
Visualizzazione delle informazioni statistiche avanzate.....	132
Salvataggio di un rapporto in un file	132
Utilizzo del filtraggio complesso	133
Ricerca eventi.....	134

SELEZIONE DI UN COMPONENTE O DI UN'ATTIVITÀ PER CREARE UN RAPPORTO

È possibile ottenere informazioni sugli eventi verificatisi durante il funzionamento di ciascun componente di Kaspersky Anti-Virus o durante l'esecuzione di attività, ad esempio Anti-Virus File, aggiornamenti e così via.

➡ *Per creare un rapporto relativo a un componente o un'attività specifica:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Rapporto** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella scheda **Rapporto**, cliccare sul bottone **Rapporto dettagliato**.
3. Nella finestra visualizzata, selezionare un componente o un'attività per cui creare un rapporto nell'elenco a discesa a sinistra. Dopo aver selezionato la voce **Protezione**, verrà creato il rapporto per tutti i componenti di protezione.

GESTIONE DEL RAGGRUPPAMENTO DELLE INFORMAZIONI NEL RAPPORTO

È possibile gestire le modalità di raggruppamento delle informazioni nel rapporto utilizzando uno dei diversi attributi disponibili. L'insieme di attributi varia in base al componente e all'attività dell'applicazione. Sono disponibili le opzioni seguenti:

- **Non raggruppare:** verranno visualizzati tutti gli eventi.
- **Raggruppa per attività:** i dati verranno raggruppati in base alle attività eseguite dai componenti di Kaspersky Anti-Virus.
- **Raggruppa per applicazione:** i dati verranno raggruppati in base alle applicazioni che mostrano attività nel sistema ed elaborati da Kaspersky Anti-Virus.
- **Raggruppa per risultato:** i dati verranno raggruppati in base ai risultati della scansione o dell'elaborazione dell'oggetto.

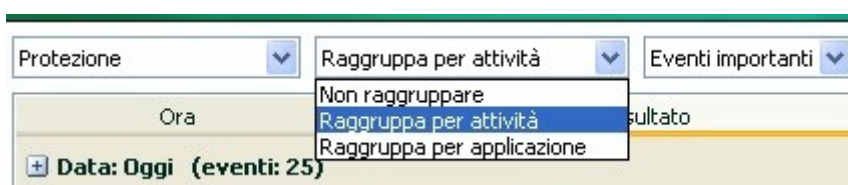


Figura 13. Attributi per il raggruppamento delle informazioni nel rapporto

Per ottenere rapidamente le informazioni desiderate e ridurre le dimensioni di raggruppamento, viene fornito un criterio di ricerca (vedere la sezione "Ricerca eventi" a pagina [134](#)). È inoltre possibile specificare un criterio di ricerca.

➡ *Per utilizzare il raggruppamento in base a un determinato attributo:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Rapporti** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella scheda **Rapporti**, cliccare sul bottone **Rapporto dettagliato**.
3. Selezionare l'attributo di raggruppamento dal menu a discesa nella finestra visualizzata.

NOTIFICA SUL COMPLETAMENTO DEL RAPPORTO

È possibile creare una pianificazione in base alla quale Kaspersky Anti-Virus notificherà all'utente quando il rapporto è pronto.

➔ *Per creare una pianificazione di notifica:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Rapporti**.
2. Nella finestra visualizzata, nella scheda **Rapporti**, selezionare la casella ☒ **Notifiche sui rapporti**. Cliccare sul collegamento con il valore temporale preimpostato.
3. Creare la pianificazione nella finestra **Pianificazione rapporti** visualizzata.

SELEZIONE DEI TIPI DI EVENTO

In un rapporto viene registrato un elenco completo di tutti gli eventi importanti che si verificano durante l'attività del componente della protezione, l'esecuzione delle scansioni o l'aggiornamento del database dell'applicazione. È possibile selezionare il tipo di evento da registrare.

Gli eventi possono appartenere a uno dei tipi seguenti:

- **Eventi critici.** Eventi di importanza fondamentale che indicano problemi riscontrati nel funzionamento di Kaspersky Anti-Virus o vulnerabilità nel sistema di protezione del computer. Includono, ad esempio, il rilevamento di un virus o un errore di funzionamento.
- **Eventi importanti.** Eventi da esaminare sempre con attenzione in quanto riflettono situazioni importanti nel funzionamento dell'applicazione, ad esempio l'evento **terminato**.

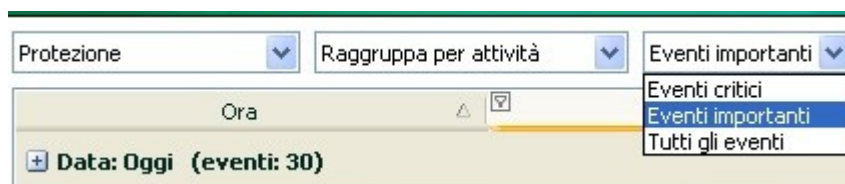


Figura 14. Selezione del tipo di evento

Se la voce **Tutti gli eventi** è selezionata, nel rapporto verranno visualizzati tutti gli eventi a condizione che le caselle corrispondenti siano selezionate nel blocco **Rapporti** della sezione **Rapporti e Backup** (vedere la sezione "Registrazione degli eventi nei rapporti" a pagina 116). Si tratta di caselle che consentono la registrazione nel rapporto di record di eventi non critici nonché di eventi del file system e del Registro di sistema. Se tali caselle non sono selezionate, vengono visualizzati un'icona di avviso e il collegamento **Disabilitato** accanto all'elenco a discesa di selezione del tipo di evento. Utilizzare il collegamento per passare alla finestra delle impostazioni dei rapporti e per selezionare le relative caselle.

➔ *Per creare un rapporto su un determinato tipo di evento:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Rapporto** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella scheda **Rapporto**, cliccare sul bottone **Rapporto dettagliato**.
3. Selezionare il tipo di evento dal menu a discesa nella finestra visualizzata. Se è necessario creare un rapporto per tutti gli eventi, selezionare il valore **Tutti gli eventi**.

VISUALIZZAZIONE DEI DATI SULLO SCHERMO

Gli eventi inclusi nel rapporto vengono visualizzati in una tabella. È possibile creare un insieme di dati per filtrare le informazioni specificando una condizione di restrizione. A tale scopo, cliccare sull'area a sinistra dell'intestazione della colonna della tabella per la quale si desidera imporre una restrizione. L'elenco a discesa visualizza i valori possibili delle condizioni di restrizione, ad esempio **Ieri** per la colonna **Ora**, **Messaggio e-mail** per la colonna **Oggetto** e così via. Selezionare il valore richiesto per ogni colonna. La query verrà eseguita in base alla condizione di restrizione specificata. Se si desidera visualizzare tutti i dati, selezionare la voce **Tutto** nell'elenco di restrizioni.

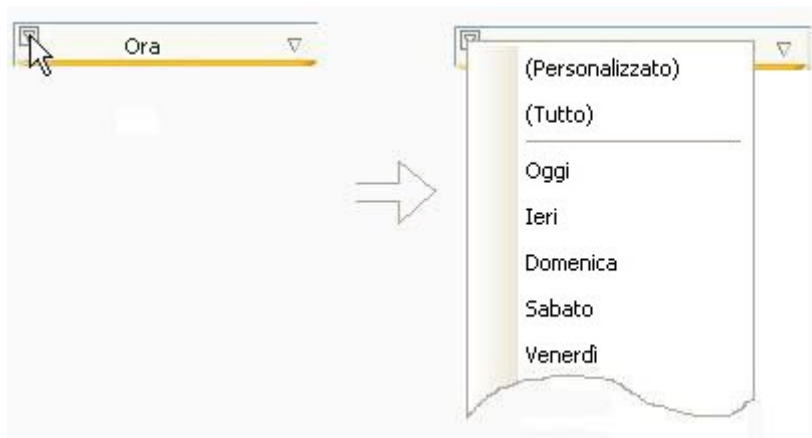


Figura 15. Specifica di una condizione di restrizione

È inoltre possibile specificare le impostazioni di una ricerca complessa sotto forma di un intervallo all'interno del quale selezionare dati su eventi passati. A tale scopo, selezionare la voce **Personalizzato** dall'elenco a discesa delle restrizioni. Nella finestra visualizzata, specificare l'intervallo temporale desiderato (vedere la sezione "Utilizzo del filtraggio complesso" a pagina [133](#)).

Per semplificare la creazione del rapporto, utilizzare il menu di scelta rapida per accedere agli attributi che consentono il raggruppamento e l'esecuzione di query sugli eventi.



Figura 16. Menu di scelta rapida

➤ *Per specificare una limitazione:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Rapporti** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella scheda **Rapporti**, cliccare sul bottone **Rapporto dettagliato**.
3. Nella finestra visualizzata, cliccare sull'area a sinistra dell'intestazione della colonna della tabella per la quale si desidera imporre una restrizione. Selezionare una restrizione richiesta nell'elenco a discesa. Se la voce **Personalizzato** è selezionata, sarà possibile specificare condizioni di filtraggio complesso (vedere la sezione "Utilizzo del filtraggio complesso" a pagina [133](#)).

➤ *Per nascondere o mostrare le colonne della tabella:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Rapporti** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella scheda **Rapporti**, cliccare sul bottone **Rapporto dettagliato**.
3. Nella finestra visualizzata, cliccare con il tasto destro del mouse sull'area a destra dell'intestazione di qualsiasi colonna di tabella. Per nascondere le colonne della tabella, deselezionare le caselle accanto ai nomi corrispondenti nel menu di scelta rapida.

VISUALIZZAZIONE DELLE INFORMAZIONI STATISTICHE AVANZATE

Nella parte inferiore della finestra del rapporto sono contenute le statistiche relative al funzionamento dell'attività o del componente selezionato di Kaspersky Anti-Virus. È possibile visualizzare le statistiche avanzate in formato grafico o tabella (in base al componente o all'attività). Utilizzare il bottone  nella parte superiore della finestra per visualizzare le statistiche avanzate. Le statistiche vengono visualizzate per il giorno corrente e per l'intero periodo durante il quale l'applicazione è rimasta installata nel computer.

➤ *Per visualizzare le statistiche avanzate, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Rapporti** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella scheda **Rapporti**, cliccare sul bottone **Rapporto dettagliato**.
3. Nella finestra visualizzata, selezionare il componente dell'applicazione in cui si intende visualizzare le statistiche avanzate e utilizzare il bottone  nella parte superiore della finestra.

SALVATAGGIO DI UN RAPPORTO IN UN FILE

Il rapporto ottenuto può essere salvato in un file.

➤ *Per farlo, eseguire le operazioni seguenti:*

1. Aprire la finestra dell'applicazione e cliccare sul collegamento **Rapporti** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella scheda **Rapporti**, cliccare sul bottone **Rapporto dettagliato**.
3. Nella finestra visualizzata creare il rapporto richiesto e cliccare sul bottone **Salva**.
4. Nella finestra visualizzata, selezionare una cartella in cui salvare il file dei rapporti e immettere il nome del file.

UTILIZZO DEL FILTRAGGIO COMPLESSO

La finestra **Filtro personalizzato** (vedere la figura sotto) consente di specificare condizioni per il filtraggio complesso dei dati, nonché criteri di ricerca dei dati per qualsiasi colonna di tabella. A titolo di esempio, verrà esaminata la procedura di utilizzo della finestra con la colonna **Ora**.

L'esecuzione di query sui dati con un filtro complesso si basa sulle funzioni di congiunzione logica (AND logico) e disgiunzione (OR logico) che è possibile utilizzare per controllare la query.

I limiti della query, in questo caso Ora, si trovano nei campi della parte destra della finestra. Per specificarli, è possibile utilizzare i tasti freccia sulla tastiera. L'elenco a discesa **Mostra righe il cui valore è** consente di scegliere la condizione per la query di eventi, ad esempio **Maggiore di** se si desidera ottenere solo i risultati che superano il valore specificato nel campo a destra.

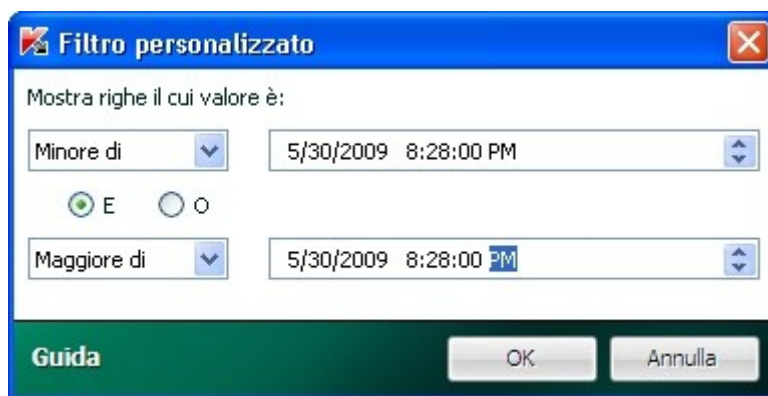


Figura 17. Specifica delle condizioni di filtraggio complesso

Se si desidera che la query dati soddisfi entrambe le condizioni specificate, selezionare **E**. Se è richiesta solo una delle due condizioni, selezionare **O**.

Per diversi tipi di dati, il limite dell'intervallo di ricerca non è un valore numerico o temporale ma una parola, ad esempio la query può restituire il valore **OK** per la colonna **Risultato**. In questo caso la parola specificata quale limite verrà confrontata con altre condizioni di parole in ordine alfabetico.

► Per specificare condizioni di filtraggio complesse:

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella scheda **Rapporti**, cliccare sul bottone **Rapporto dettagliato**.
3. Nella finestra visualizzata cliccare sull'area a sinistra della colonna di tabella per la quale si desidera specificare condizioni di filtraggio complesso. Selezionare la voce **Personalizzato** dal menu a discesa. È inoltre possibile selezionare la voce **Filtra per questo campo** nel menu di scelta rapida (vedere la sezione "Visualizzazione dei dati sullo schermo" a pagina [130](#)) che viene visualizzato dopo aver cliccato con il pulsante destro del mouse sulla colonna desiderata nella tabella.
4. Nella finestra **Filtro personalizzato** visualizzata, specificare le condizioni di filtraggio desiderate.

RICERCA EVENTI

Questa finestra (vedere la figura in basso) è stata progettata per consentire la ricerca degli eventi verificatisi nel sistema ed elaborati da Kaspersky Anti-Virus.

Di seguito vengono descritti i concetti utilizzati per lavorare con questa finestra.

- Il campo **Stringa** viene utilizzato per immettere la parola chiave, ad esempio explorer. Per avviare la ricerca, cliccare sul bottone **Trova successivo**. La ricerca dei dati desiderati può richiedere tempo. Una volta completata la ricerca, gli eventi relativi alla parola chiave inserita verranno visualizzati. Cliccando sul bottone **Contrassegna tutto** vengono selezionate tutte le voci trovate corrispondenti alla parola chiave di ricerca.
- Il campo **Colonna** consente di selezionare la colonna della tabella in base alla quale verrà eseguita la ricerca della parola chiave. Questa selezione consente di risparmiare il tempo richiesto per eseguire una ricerca (a meno che, naturalmente, non sia stato selezionato il valore **Tutto**).



Figura 18. ricerca eventi

Per effettuare una ricerca sensibile alle maiuscole/minuscole, selezionare la casella ☒ **Maiuscole/minuscole**. La casella ☒ **Solo parole intere** consente di restringere la ricerca alle sole parole intere.

➡ *Per utilizzare la ricerca eventi:*

1. Aprire la finestra principale dell'applicazione e cliccare sul collegamento **Rapporti** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella scheda **Rapporti**, cliccare sul bottone **Rapporto dettagliato**.
3. Nella finestra visualizzata, cliccare con il tasto destro del mouse sull'area a destra dell'intestazione di qualsiasi colonna di tabella. Scegliere la voce **Cerca** dal menu di scelta rapida.
4. Specificare i criteri di ricerca nella finestra **Cerca** visualizzata.

NOTIFICHE

Quando si verificano eventi di runtime di Kaspersky Anti-Virus, vengono visualizzati messaggi di notifica speciali. A seconda della criticità dell'evento per la protezione del computer, potrebbero essere visualizzati i tipi di notifica seguenti:

- **Allarme.** Si è verificato un evento critico, ad esempio è stato rilevato un oggetto dannoso o un'attività pericolosa nel sistema. È necessario decidere subito come affrontare la minaccia. La finestra di notifica di questo tipo è di colore rosso.
- **Attenzione.** Si è verificato un evento potenzialmente pericoloso. Ad esempio, nel sistema sono stati rilevati file potenzialmente infetti o un'attività sospetta. È necessario stabilire quanto è pericolosa l'azione in questione. La finestra di notifica di questo tipo è di colore giallo.
- **Informazioni.** Questa notifica fornisce informazioni su eventi non critici. La finestra di notifica di questo tipo è di colore verde.

La finestra di notifica si compone di quattro parti:

1. *Intestazione della finestra.* L'intestazione della finestra di notifica contiene una breve descrizione dell'evento, ad esempio: richiesta di diritti, attività sospetta, nuova rete, avviso, virus.
2. *Descrizione dell'evento.* La sezione di descrizione dell'evento visualizza informazioni dettagliate sul motivo della visualizzazione della notifica: nome dell'applicazione che ha causato l'evento, nome della minaccia individuata, impostazioni della connessione di rete individuata e così via.
3. *Area di selezione dell'azione.* In questa sezione è possibile selezionare una delle azioni disponibili per l'evento. Le opzioni suggerite per l'azione dipendono dal tipo di evento, ad esempio: **Disinfetta**, **Elimina**, **Ignora** – se è stato individuato un virus, **Consenti**, **Blocca** – se l'applicazione richiede diritti per l'esecuzione di azioni potenzialmente dannose. L'azione consigliata dagli esperti di Kaspersky Lab verrà visualizzata in grassetto.

Se si seleziona **Consenti** o **Blocca**, la finestra verrà aperta e sarà possibile selezionare *la modalità di applicazione dell'azione*. Per l'azione **Consenti** è possibile selezionare una delle modalità seguenti:

- **Consenti sempre.** Selezionare questa opzione per consentire le attività del programma apportando modifiche alla regola di accesso del programma alle risorse di sistema.
- **Consenti ora.** Selezionare questa casella per applicare l'azione selezionata a tutti gli eventi analoghi rilevati durante la sessione dell'applicazione. La sessione dell'applicazione è l'intervallo tra il relativo avvio e il momento in cui è stata arrestata o riavviata.
- **Rendi attendibile.** Selezionare questa opzione per spostare l'applicazione nel gruppo **Attendibili**.

Per l'azione **Blocca** è possibile selezionare una delle modalità seguenti:

- **Blocca sempre.** Selezionare questa opzione per bloccare le attività del programma apportando modifiche alla regola di accesso del programma alle risorse di sistema.
- **Blocca ora.** Selezionare questa casella per applicare l'azione selezionata a tutti gli eventi analoghi rilevati durante la sessione dell'applicazione. La sessione dell'applicazione è l'intervallo tra il relativo avvio e il momento in cui è stata arrestata o riavviata.
- **Termina.** Selezionare questa opzione per interrompere il funzionamento del programma.

4. *Area di selezione di ulteriori azioni.* Questa sezione consente di selezionare un'azione ulteriore:

- **Aggiungi alle esclusioni.** Se si è certi che l'oggetto rilevato non sia dannoso, si consiglia di aggiungerlo all'area attendibile per evitare che il programma rilevi falsi positivi ripetuti durante l'utilizzo dell'oggetto.
- **Applica a tutti gli oggetti.** Selezionare questa casella per fare in modo che l'azione specificata venga applicata a tutti gli oggetti con lo stesso stato in situazioni analoghe.

IN QUESTA SEZIONE:

Rilevamento di un oggetto dannoso	136
Impossibile disinfettare l'oggetto.....	137
Richiesta di esecuzione di una procedura speciale	137
Rilevamento di un oggetto pericoloso nel traffico	137
Rilevamento di un oggetto sospetto	138
Rilevamento di un'attività pericolosa nel sistema	139
Rilevamento di processi nascosti	139
Rilevamento di un tentativo di accesso al Registro di sistema	140
Rilevamento di un attacco di phishing	140
Rilevamento di un collegamento sospetto	141
Rilevamento di un certificato non valido	141

RILEVAMENTO DI UN OGGETTO DANNOSO

Se Anti-Virus File, Anti-Virus Posta o una scansione anti-virus rileva un codice dannoso, viene visualizzata una notifica speciale.

Tale notifica indica:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto dannoso così come è elencato nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.
- Il nome completo dell'oggetto dannoso e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Disinfetta:** viene eseguito un tentativo di disinfezione dell'oggetto dannoso. Prima del trattamento, viene eseguita una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Elimina:** l'oggetto dannoso viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Ignora:** l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

Successivamente sarà possibile tornare agli oggetti dannosi ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella ☒ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al relativo completamento.

IMPOSSIBILE DISINFETTARE L'OGGETTO

In alcuni casi può risultare impossibile disinfettare un oggetto dannoso. Questo può succedere se un file è talmente danneggiato che è impossibile eliminarne il codice dannoso e ripristinarne l'integrità. La procedura per il trattamento di questi casi non può essere applicata a diversi tipi di oggetti pericolosi, ad esempio i Trojan.

In queste situazioni verrà visualizzata una notifica speciale con le informazioni seguenti:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto dannoso così come è elencato nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.
- Il nome completo dell'oggetto dannoso e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Elimina:** l'oggetto dannoso viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Ignora:** l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

Successivamente sarà possibile tornare agli oggetti dannosi ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella ☒ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di un'attività di scansione anti-virus fino al relativo completamento.

RICHIESTA DI ESECUZIONE DI UNA PROCEDURA SPECIALE

Quando viene rilevata una minaccia attualmente attiva nel sistema, ad esempio un processo dannoso nella RAM o negli oggetti di avvio, viene visualizzato un messaggio per richiedere l'esecuzione di una speciale procedura avanzata di disinfezione.

Gli specialisti di Kaspersky Lab consigliano di accettare l'esecuzione di tale procedura avanzata. A tale scopo, cliccare sul bottone **OK**. Tenere presente, tuttavia, che il computer verrà riavviato al termine della procedura e pertanto si consiglia di salvare il lavoro corrente e chiudere tutte le applicazioni prima di eseguire la procedura.

Durante l'esecuzione della procedura di disinfezione, non è possibile avviare sessioni di modifica del Registro del sistema operativo o del client di posta. Dopo aver riavviato il computer, viene consigliata l'esecuzione di una scansione anti-virus completa.

RILEVAMENTO DI UN OGGETTO PERICOLOSO NEL TRAFFICO

Quando Anti-Virus Web rileva un oggetto dannoso nel traffico, viene visualizzata una notifica speciale.

La notifica contiene le informazioni seguenti:

- Il tipo di minaccia, ad esempio *variante virus*, e il nome dell'oggetto pericoloso così come è elencato nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome dell'oggetto viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata.
- Il nome completo dell'oggetto pericoloso con il percorso della pagina Web.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Consenti:** il download dell'oggetto continua.
- **Blocca:** il download dell'oggetto dalla risorsa Web viene bloccato.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella ☒ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al relativo completamento.

RILEVAMENTO DI UN OGGETTO SOSPETTO

Se Anti-Virus File, Anti-Virus Posta o una scansione anti-virus rileva un oggetto contenente codice di un virus sconosciuto o codice modificato di un virus noto, viene visualizzata una notifica speciale.

Tale notifica indica:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto così come è elencato nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.
- Il nome completo dell'oggetto e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Quarantena** – l'oggetto viene messo in Quarantena. Quando si mette un oggetto in Quarantena, l'oggetto viene spostato e non copiato. Esso viene eliminato dal disco o dalla posta elettronica e salvato nella cartella Quarantena. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

Successivamente, quando si esegue la scansione degli oggetti in Quarantena con firme delle minacce aggiornate, lo stato dell'oggetto potrebbe cambiare. L'oggetto può ad esempio essere identificato come infetto ed essere elaborato utilizzando un database aggiornato. In caso contrario, è possibile assegnare all'oggetto lo stato *non infetto* e quindi ripristinarlo.

Se un file viene messo in quarantena manualmente e dopo una successiva scansione risulta non infetto, lo stato non passerà a OK immediatamente dopo la scansione. Questo si verificherà solo se la scansione è stata eseguita dopo un determinato intervallo di tempo (almeno tre giorni) in seguito alla messa in quarantena del file.

- **Elimina:** l'oggetto viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Ignora:** l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

Successivamente sarà possibile tornare agli oggetti ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella ☒ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al relativo completamento.

Se si è certi che l'oggetto rilevato non sia dannoso, si consiglia di aggiungerlo all'area attendibile per evitare che il programma rilevi falsi positivi ripetuti durante l'utilizzo dell'oggetto.

RILEVAMENTO DI UN'ATTIVITÀ PERICOLOSA NEL SISTEMA

Quando Difesa Proattiva rileva nel sistema un'attività pericolosa dell'applicazione, viene visualizzata una notifica speciale con le informazioni seguenti:

- Il nome della minaccia così come è elencata nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome della minaccia viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata.
- Il nome completo del file del processo che ha avviato l'attività pericolosa e il relativo percorso.
- Risposte possibili:
 - **Quarantena:** il processo viene arrestato e il file eseguibile viene messo in Quarantena. Quando si mette un oggetto in Quarantena, l'oggetto viene spostato e non copiato. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

Successivamente, quando si esegue la scansione degli oggetti in Quarantena con firme delle minacce aggiornate, lo stato dell'oggetto potrebbe cambiare. L'oggetto può ad esempio essere identificato come infetto ed essere elaborato utilizzando un database aggiornato. In caso contrario, è possibile assegnare all'oggetto lo stato *non infetto* e quindi ripristinarlo.

Se un file viene messo in quarantena manualmente e dopo una successiva scansione risulta non infetto, lo stato non passerà a OK immediatamente dopo la scansione. Questo si verificherà solo se la scansione è stata eseguita dopo un determinato intervallo di tempo (almeno tre giorni) in seguito alla messa in quarantena del file.

- **Termina:** arresta il processo.
- **Consenti:** consente l'esecuzione del processo.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella ☒ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al relativo completamento.

Se si è certi che il programma rilevato non sia pericoloso, si consiglia di aggiungerlo all'area attendibile per evitare che Kaspersky Anti-Virus generi falsi positivi ripetuti quando lo rileva.

RILEVAMENTO DI PROCESSI NASCOSTI

Quando Difesa Proattiva rileva nel sistema un'attività nascosta, viene visualizzata una notifica speciale con le informazioni seguenti:

- Il nome della minaccia così come è elencata nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome della minaccia viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata.
- Il nome completo del file del processo nascosto e il relativo percorso.
- Risposte possibili:
 - **Quarantena** – il file eseguibile del processo viene messo in Quarantena. Quando si mette un oggetto in Quarantena, l'oggetto viene spostato e non copiato. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

Successivamente, quando si esegue la scansione degli oggetti in Quarantena con firme delle minacce aggiornate, lo stato dell'oggetto potrebbe cambiare. L'oggetto può ad esempio essere identificato come infetto ed essere elaborato utilizzando un database aggiornato. In caso contrario, è possibile assegnare all'oggetto lo stato *non infetto* e quindi ripristinarlo.

Se un file viene messo in quarantena manualmente e dopo una successiva scansione risulta non infetto, lo stato non passerà a **OK** immediatamente dopo la scansione. Questo si verificherà solo se la scansione è stata eseguita dopo un determinato intervallo di tempo (almeno tre giorni) in seguito alla messa in quarantena del file.

- **Termina:** arresta il processo.
- **Consenti:** consente l'esecuzione del processo.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella ☒ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al relativo completamento.

Se si è certi che il programma rilevato non sia pericoloso, si consiglia di aggiungerlo all'area attendibile per evitare che Kaspersky Anti-Virus generi falsi positivi ripetuti quando lo rileva.

RILEVAMENTO DI UN TENTATIVO DI ACCESSO AL REGISTRO DI SISTEMA

Quando Difesa Proattiva rileva un tentativo di accesso alle chiavi del Registro di sistema, viene visualizzata una notifica speciale con le informazioni seguenti:

- La chiave del Registro di sistema alla quale si sta tentando di accedere.
- Il nome completo del file del processo che ha avviato il tentativo di accesso alle chiavi del Registro di sistema e il relativo percorso.
- Risposte possibili:
 - **Consenti:** l'esecuzione dell'azione pericolosa viene consentita una volta;
 - **Blocca:** l'azione pericolosa viene bloccata una volta.

Per eseguire l'azione selezionata automaticamente ogni volta che l'attività viene avviata nel computer, selezionare la casella

☒ **Crea una regola.**

Se si è certi che le attività eseguite dall'applicazione che ha tentato di accedere alle chiavi del Registro di sistema non siano pericolose, aggiungere l'applicazione all'elenco di applicazioni attendibili.

RILEVAMENTO DI UN ATTACCO DI PHISHING

Ogni volta che Kaspersky Anti-Virus rileva un attacco di phishing, viene visualizzata una notifica speciale.

Tale notifica contiene le informazioni seguenti:

- Il nome della minaccia (*attacco di phishing*) come collegamento all'Enciclopedia dei Virus di Kaspersky Lab con una panoramica dettagliata della minaccia stessa.
- L'indirizzo Web dell'attacco di phishing.
- Risposte possibili:
 - **Consenti:** il download dal sito di phishing continua.
 - **Blocca:** il download dal sito di phishing viene bloccato.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella  **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al relativo completamento.

RILEVAMENTO DI UN COLLEGAMENTO SOSPETTO

Ogni volta che Kaspersky Anti-Virus rileva un tentativo di apertura di un sito Web, il cui indirizzo è contenuto nell'elenco di indirizzi Web sospetti, viene visualizzata una notifica speciale a comparsa.

La notifica contiene le informazioni seguenti:

- Indirizzo del sito Web.
- Risposte possibili:
 - **Consenti**: il download dal sito Web continua.
 - **Blocca**: il download dal sito Web viene bloccato.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella  **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al relativo completamento.

RILEVAMENTO DI UN CERTIFICATO NON VALIDO

Il controllo di protezione per la connessione mediante il protocollo SSL viene eseguito utilizzando il certificato installato. Se viene rilevato un certificato non valido quando si tenta di stabilire la connessione al server, ad esempio se il certificato viene sostituito da un intruso, viene visualizzata una notifica.

La notifica conterrà le informazioni sulla possibile causa dell'errore e identificherà l'indirizzo e la porta remoti. Verrà richiesto di decidere se continuare o meno la connessione con un certificato non valido:

- **Accetta certificato**: la connessione al sito Web continua;
- **Nega certificato**: la connessione al sito Web viene interrotta;
- **Visualizza certificato**: vengono visualizzate informazioni sul certificato.

CONVALIDA DELLE IMPOSTAZIONI DI KASPERSKY ANTI-VIRUS

Dopo aver installato e configurato Kaspersky Anti-Virus, è possibile verificare la correttezza della configurazione tramite un virus di "prova" e le sue varianti. Per ciascun protocollo/componente di protezione è necessario eseguire un test separato.

IN QUESTA SEZIONE:

"Virus" di prova EICAR e sue varianti	142
Test della protezione del traffico HTTP	143
Test della protezione del traffico SMTP	143
Convalida delle impostazioni di Anti-Virus File	144
Convalida delle impostazioni dell'attività di scansione anti-virus	144

"VIRUS" DI PROVA EICAR E SUE VARIANTI

Questo "virus" di prova è stato progettato specificamente da  (European Institute for Computer Antivirus Research) per il collaudo dei prodotti anti-virus.

Il "virus" di prova NON È UN VIRUS, poiché non contiene codice in grado di danneggiare il computer. Tuttavia, la maggior parte dei prodotti anti-virus lo identifica come tale.

Si raccomanda di non utilizzare mai virus autentici per verificare il corretto funzionamento di un programma anti-virus.

È possibile scaricare il "virus" di prova dal sito Web ufficiale di **EICAR** all'indirizzo http://www.eicar.org/anti_virus_test_file.htm.

Prima di scaricare il file, è necessario disabilitare la protezione anti-virus del computer perché altrimenti l'applicazione identificherà ed elaborerà il file *anti_virus_test_file.htm* come oggetto infetto trasferito tramite il protocollo HTTP. Riattivare la protezione anti-virus subito dopo aver scaricato il "virus" di prova.

L'applicazione identifica il file scaricato dal sito **EICAR** come oggetto infetto contenente un virus che **non può essere disinfettato** ed esegue le azioni specificate per questo tipo di oggetto.

È possibile inoltre utilizzare varianti del "virus" di prova standard per verificare il funzionamento dell'applicazione. A tal fine, modificare il contenuto del "virus" standard aggiungendo uno dei prefissi elencati nella tabella di seguito. Per modificare il "virus" di prova, è possibile utilizzare qualsiasi editor di testo o di ipertesto, ad esempio **Blocco note Microsoft**, **UltraEdit32** e così via.

È possibile verificare il corretto funzionamento dell'applicazione anti-virus tramite il "virus" modificato EICAR solo se i database anti-virus sono stati aggiornati il 24 ottobre 2003 o successivamente (Ottobre 2003, aggiornamenti cumulativi).

Nella tabella seguente la prima colonna contiene i prefissi che devono essere aggiunti all'inizio della stringa per un "virus" di prova standard. La seconda colonna elenca tutti i valori possibili dello stato che l'applicazione Anti-Virus può assegnare all'oggetto in base ai risultati della scansione. La terza colonna indica come vengono elaborati gli oggetti con lo stato specificato. Si noti che le azioni effettive eseguite sugli oggetti sono determinate dalle impostazioni dell'applicazione.

Dopo aver aggiunto un prefisso al "virus" di prova, salvare il nuovo file con un nome diverso, ad esempio: *eicar_dele.com*. Assegnare nomi simili a tutti i "virus" modificati.

Table 1. Varianti del "virus" di prova

Prefisso	Stato dell'oggetto	Informazioni di elaborazione dell'oggetto
Nessun prefisso, "virus" di prova standard.	Infetto. L'oggetto contiene codice di un virus noto e non può essere disinfettato.	L'applicazione identifica l'oggetto come virus non disinfettabile. Si verifica un errore al tentativo di disinfettare l'oggetto; verrà eseguita l'azione specificata per gli oggetti non disinfettabili.
CORR-	Danneggiato.	L'applicazione ha potuto accedere all'oggetto ma non ha potuto esaminarlo, poiché l'oggetto è danneggiato, ad esempio la struttura del file è danneggiata o il formato file non è valido. Informazioni sull'elaborazione dell'oggetto sono disponibili nel rapporto sul funzionamento dell'applicazione.
WARN-	Sospetto. L'oggetto contiene codice di un virus sconosciuto e non può essere disinfettato.	L'oggetto è stato ritenuto sospetto dall'analizzatore euristico di codice. Al momento del rilevamento, i database delle firme delle minacce di Anti-Virus non contengono alcuna descrizione della procedura per il trattamento di questo oggetto. Il rilevamento di un oggetto di questo tipo viene notificato.
SUSP-	Sospetto. L'oggetto contiene codice modificato di un virus noto e non può essere disinfettato.	L'applicazione ha rilevato una corrispondenza parziale tra una sezione del codice dell'oggetto e una sezione di codice di un virus noto. Al momento del rilevamento, i database delle firme delle minacce di Anti-Virus non contengono alcuna descrizione della procedura per il trattamento di questo oggetto. Il rilevamento di un oggetto di questo tipo viene notificato.
ERRO-	Errore di scansione.	Si è verificato un errore durante la scansione di un oggetto. L'applicazione non ha potuto eseguire l'accesso all'oggetto, in quanto l'integrità dell'oggetto è stata compromessa, ad esempio a causa di un archivio in più volumi, o non è stata stabilita una connessione a esso, ad esempio se l'oggetto viene esaminato in una risorsa di rete. Informazioni sull'elaborazione dell'oggetto sono disponibili nel rapporto sul funzionamento dell'applicazione.
CURE-	Infetto. L'oggetto contiene codice di un virus noto e può essere disinfettato.	L'oggetto contiene un virus che può essere disinfettato. L'applicazione disinfetterà l'oggetto; il testo del corpo del "virus" verrà sostituito dalla parola CURE. Il rilevamento di un oggetto di questo tipo viene notificato.
DELE-	Infetto. L'oggetto contiene codice di un virus noto e non può essere disinfettato.	L'applicazione identifica l'oggetto come virus non disinfettabile. Si verifica un errore al tentativo di disinfettare l'oggetto; verrà eseguita l'azione specificata per gli oggetti non disinfettabili. Il rilevamento di un oggetto di questo tipo viene notificato.

TEST DELLA PROTEZIONE DEL TRAFFICO HTTP

► Per verificare che i virus siano stati rilevati correttamente nel flusso di dati trasferito attraverso il protocollo HTTP, eseguire le operazioni seguenti:

Provare a scaricare questo "virus" di prova dal sito Web ufficiale di **EICAR** all'indirizzo http://www.eicar.org/anti_virus_test_file.htm.

Quando il computer tenta di scaricare il "virus" di prova, Kaspersky Anti-Virus rileva questo oggetto identificandolo come oggetto infetto impossibile da disinfettare, ed esegue l'azione specificata nelle impostazioni di scansione del traffico HTTP per gli oggetti che presentano questo stato. Per impostazione predefinita, quando si tenta di scaricare il "virus" di prova, la connessione al sito Web viene terminata e nel browser viene visualizzato un messaggio che informa l'utente che l'oggetto è stato infettato dal virus EICAR-Test-File.

TEST DELLA PROTEZIONE DEL TRAFFICO SMTP

Per rilevare i virus presenti nei flussi dati trasferiti tramite il protocollo SMTP, è necessario utilizzare un sistema di posta elettronica che utilizzi questo protocollo per trasferire i dati.

Si consiglia di verificare in che modo Anti-Virus gestisca i messaggi di posta elettronica in uscita, inclusi il corpo del messaggio e gli allegati. Per testare la funzione di rilevamento dei virus nel corpo del messaggio, copiare il testo del "virus" di prova standard o di quello modificato nel corpo del messaggio.

➡ *Per farlo:*

1. Creare un messaggio in formato **testo normale** tramite un client di posta elettronica installato nel computer.

Se creato in formato RTF o HTML, un messaggio contenente un virus di prova non verrà esaminato.

2. Copiare il testo del "virus" standard o modificato all'inizio del messaggio o allegare al messaggio un file contenente il "virus" di prova.
3. Inviare il messaggio all'amministratore.

L'applicazione individuerà l'oggetto, lo identificherà come infetto e lo bloccherà.

CONVALIDA DELLE IMPOSTAZIONI DI ANTI-VIRUS FILE

➡ *Per verificare che la configurazione di Anti-Virus File sia corretta:*

1. Creare una cartella su disco. Copiare nella cartella il "virus" di prova scaricato dal sito Web ufficiale di **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) e tutte le varianti create.
2. Lasciare che tutti gli eventi vengano registrati, in modo che il file del rapporto conservi i dati sugli oggetti danneggiati o su quelli non esaminati a causa di errori.
3. Eseguire il virus "di prova" o una delle relative versioni modificate.

Anti-Virus File intercetta la chiamata per eseguire il file, la esamina ed esegue l'azione specificata nelle impostazioni per gli oggetti che presentano quello stato. Selezionando diverse azioni da eseguire sull'oggetto rilevato, è possibile effettuare un controllo completo del funzionamento del componente.

Il rapporto sul funzionamento del componente include informazioni sui risultati dell'operazione eseguita da Anti-Virus File.

CONVALIDA DELLE IMPOSTAZIONI DELL'ATTIVITÀ DI SCANSIONE ANTI-VIRUS

➡ *Per verificare che l'attività di scansione anti-virus sia configurata correttamente:*

1. Creare una cartella su disco. Copiare nella cartella il "virus" di prova scaricato dal sito Web ufficiale di **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) e tutte le varianti create.
2. Creare una nuova attività di scansione anti-virus e selezionare la cartella contenente il gruppo di "virus" di prova come oggetto da esaminare.
3. Lasciare che tutti gli eventi vengano registrati, in modo che il file del rapporto conservi i dati sugli oggetti danneggiati e su quelli non esaminati a causa di errori.
4. Eseguire l'attività di scansione anti-virus.

Quando l'attività di scansione è in esecuzione, le azioni specificate nelle impostazioni verranno eseguite al rilevamento di oggetti infetti o sospetti. Selezionando diverse azioni da eseguire sull'oggetto rilevato, è possibile effettuare un controllo completo del funzionamento del componente.

È possibile visualizzare tutte le informazioni sulle azioni dell'attività di scansione anti-virus nel rapporto sul funzionamento del componente.

UTILIZZO DELL'APPLICAZIONE DALLA RIGA DI COMANDO

Kaspersky Anti-Virus può essere utilizzato anche dalla riga di comando. In tal caso sono consentite le operazioni seguenti:

- avvio e arresto dell'attività dei componenti dell'applicazione;
- avvio e arresto delle attività di scansione anti-virus;
- acquisizione di informazioni sullo stato corrente dei componenti e sulle relative attività e statistiche;
- scansione di oggetti selezionati;
- aggiornamento dei database e dei moduli dell'applicazione;
- richiamo della Guida nella sintassi del prompt dei comandi;
- richiamo della Guida nella sintassi dei comandi.

Sintassi del prompt dei comandi:

```
avp.com <comando> [opzioni]
```

È necessario accedere all'applicazione dalla riga di comando dalla cartella di installazione del programma o specificando il percorso completo di avp.com.

Sono disponibili i comandi seguenti:

ACTIVATE	Attiva Kaspersky Anti-Virus tramite Internet utilizzando un codice di attivazione
ADDKEY	Attiva l'applicazione tramite un file chiave. Il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia dell'applicazione.
START	Avvia un componente o un'attività.
STOP	Arresta un componente o un'attività. Il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia di Kaspersky Anti-Virus.
STATUS	Visualizza lo stato del componente o dell'attività corrente.
STATISTICS	Visualizza sullo schermo le statistiche del componente o dell'attività.
HELP	Fornisce indicazioni sulla sintassi dei comandi e sull'elenco dei comandi.
SCAN	Esegue la scansione anti-virus degli oggetti.
UPDATE	Avvia l'aggiornamento dell'applicazione.
ROLLBACK	Esegue il rollback dell'ultimo aggiornamento di Kaspersky Anti-Virus. Il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia dell'applicazione.

EXIT	Chiude l'applicazione. Il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia dell'applicazione.
IMPORT	Importa le impostazioni di protezione dell'applicazione. Il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia di Kaspersky Anti-Virus.
EXPORT	Esporta le impostazioni di protezione dell'applicazione.

Ogni comando richiede un insieme specifico di parametri.

IN QUESTA SEZIONE:

Gestione dei componenti e delle attività dell'applicazione	146
Scansione anti-virus	148
Aggiornamento dell'applicazione	151
Rollback dell'ultimo aggiornamento	151
Esportazione delle impostazioni di protezione.....	152
Importazione delle impostazioni di protezione.....	152
Avvio dell'applicazione	152
Arresto dell'applicazione.....	153
Creazione di un file di traccia	153
Visualizzazione della Guida.....	153
Codici restituiti della riga di comando	154

GESTIONE DEI COMPONENTI E DELLE ATTIVITÀ DELL'APPLICAZIONE

Sintassi del comando:

```
avp.com <comando> <profilo|nome_attività> [/R[A]:<file_rapporti>]
avp.com STOP|PAUSE <profilo|nome_attività> /password=<password>
[/R[A]:<file_rapporti>]
```

<comando>	È possibile gestire i componenti e le attività di Kaspersky Anti-Virus dalla riga di comando con i comandi seguenti: START: avvia un'attività o un componente di protezione. STOP: arresta un'attività o un componente di protezione. STATUS: visualizza lo stato corrente di un'attività o di un componente di protezione. STATISTICS: visualizza le statistiche relative a un'attività o a un componente di protezione. Il comando STOP non verrà accettato senza l'immissione di una password.
------------------------	---

<profilo nome_attività>	Come valore di <profilo> è possibile specificare qualsiasi componente di protezione di Kaspersky Anti-Virus, modulo di componente, attività di scansione o di aggiornamento a richiesta (i valori standard utilizzati nell'applicazione sono visualizzati nella tabella che segue). Come valore di <nome_attività> è possibile specificare il nome di qualsiasi attività di scansione o di aggiornamento a richiesta.
<password>	Password dell'applicazione specificata nell'interfaccia.
/R[A]:<file_rapporti>	/R:<file_rapporti>: registra solo eventi importanti nel rapporto. /RA:<report_file> – registra tutti gli eventi nel rapporto. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

L'impostazione **<profilo>** può presentare uno dei valori seguenti:

RTP	Tutti i componenti di protezione. Il comando avp.com START RTP esegue tutti i componenti di protezione se la protezione è stata completamente disabilitata. Se il componente è stato disabilitato tramite il comando STOP dalla riga di comando, non verrà riavviato dal comando avp.com START RTP. Per avviarlo, è necessario eseguire il comando avp.com START <profilo> immettendo per <profilo> il nome del componente di protezione specifico. Ad esempio, avp.com START FM.
pdm	Difesa Proattiva
FM	Anti-Virus File
EM	Anti-Virus Posta
WM	Anti-Virus Web Valori per i componenti secondari di Anti-Virus Web: httpscan (HTTP): esamina il traffico HTTP; sc: esamina gli script.
IM	Anti-Virus IM
Updater	Aggiornamento
Rollback	Rollback dell'ultimo aggiornamento
Scan_My_Computer	Scansione del computer
Scan_Objects	Scansione degli oggetti
Scan_Quarantine	Scansione della quarantena
Scan_Rootkits	Ricerca di rootkit
Scan_Startup (STARTUP)	Scansione degli oggetti di avvio
Scan_Vulnerabilities (SECURITY)	Scansione Vulnerabilità

I componenti e le attività avviati dalla riga di comando vengono eseguiti con le impostazioni configurate nell'interfaccia dell'applicazione.

Esempi:

➤ Per abilitare il componente Anti-Virus File, digitare quanto segue alla riga di comando:

```
avp.com START FM
```

➤ Per riavviare Filtro Genitori, digitare quanto segue alla riga di comando:

```
avp.com RESUME ParCtl
```

➤ Per arrestare un'attività di scansione del computer dalla riga di comando, immettere:

```
avp.com STOP Scan_My_Computer /password=<password>
```

SCANSIONE ANTI-VIRUS

L'avvio della scansione anti-virus di una determinata area e l'elaborazione degli oggetti dannosi dalla riga di comando generalmente presenta la sintassi seguente:

```
avp.com SCAN [<oggetto da esaminare>] [<azione>] [<tipi file>] [<esclusioni>] [<file configurazione>] [<impostazioni rapporti>] [<impostazioni avanzate>]
```

Per esaminare gli oggetti, è inoltre possibile utilizzare le attività create nell'applicazione avviando quella richiesta dalla riga di comando. L'attività viene eseguita con le impostazioni specificate nell'interfaccia di Kaspersky Anti-Virus.

Descrizione delle impostazioni:

<oggetto da esaminare>: questo parametro fornisce l'elenco di oggetti che verranno esaminati per rilevare eventuale codice dannoso.

Può includere diversi valori dell'elenco fornito separati da spazi.

<file>	Elenco di percorsi dei file e/o delle cartelle da esaminare. È possibile indicare un percorso assoluto o relativo. Gli elementi dell'elenco devono essere separati da uno spazio. Commenti: - Se il nome dell'oggetto contiene uno spazio, esso deve essere incluso tra virgolette. - Se viene fatto riferimento a una cartella specifica, verranno esaminati tutti i file in essa contenuti.
/MEMORY	Oggetti RAM.
/STARTUP	Oggetti di avvio.
/MAIL	Caselle di posta.
/REMDRIVES	Tutte le unità rimovibili.
/FIXDRIVES	Tutte le unità interne.
/NETDRIVES	Tutte le unità di rete.
/QUARANTINE	Oggetti in quarantena.

/ALL	Scansione completa del computer.
/@:<filelist.lst>	Percorso del file contenente un elenco di oggetti e cataloghi da esaminare. Il file deve essere in formato testo e ogni oggetto della scansione deve essere elencato in una riga separata. È possibile indicare un percorso assoluto o relativo. Il percorso deve essere inserito tra virgolette anche se contiene spazi.
<azione>: questo parametro determina le azioni che verranno eseguite sugli oggetti dannosi rilevati durante la scansione. Se non è definito, l'azione predefinita è quella con il valore /i8. Se si lavora in modalità automatica, Kaspersky Anti-Virus applicherà automaticamente l'azione consigliata dagli specialisti di Kaspersky Lab quando vengono rilevati oggetti pericolosi. Le azioni corrispondenti al valore del parametro <azione> verranno ignorate.	
/i0	Nessuna azione sull'oggetto; solo registrazione delle informazioni nel rapporto.
/i1	Gli oggetti infetti vengono elaborati e, se la disinfezione è impossibile, vengono ignorati.
/i2	Gli oggetti infetti vengono elaborati e, se la disinfezione non riesce, vengono eliminati. Non vengono eliminati gli oggetti infetti appartenenti a oggetti composti. Per impostazione predefinita, vengono eliminati gli oggetti composti con intestazione eseguibile (archivi sfx).
/i3	Gli oggetti infetti vengono elaborati e, se la disinfezione non riesce, vengono eliminati. Vengono eliminati tutti gli oggetti composti se non è possibile eliminare le parti infette.
/i4	Vengono eliminati gli oggetti infetti. Vengono eliminati tutti gli oggetti composti se non è possibile eliminare le parti infette.
/i8	Viene richiesto l'intervento dell'utente se viene rilevato un oggetto infetto.
/i9	Viene richiesto l'intervento dell'utente al termine della scansione.
<tipi file>: questo parametro definisce i tipi di file che verranno sottoposti alla scansione anti-virus. Per impostazione predefinita, questo parametro non è specificato e sono sottoposti a scansione solo i file infetti in base al contenuto.	
/fe	Vengono esaminati solo i file infetti in base all'estensione.
/fi	Vengono esaminati solo i file infetti in base al contenuto.
/fa	Vengono esaminati tutti i file.
<esclusioni>: questo parametro definisce gli oggetti esclusi dalla scansione. Può includere diversi valori dell'elenco fornito separati da spazi.	
-e:a	Non vengono esaminati gli archivi.
-e:b	Non vengono esaminati i database della posta.
-e:m	Non vengono esaminati i messaggi di posta con testo semplice.
-e:<mascherafile>	Non vengono esaminati gli oggetti corrispondenti alla maschera.
-e:<secondi>	Vengono ignorati gli oggetti la cui scansione richiede un intervallo di tempo superiore a quello specificato nel parametro <secondi> .

-es:<dimensione>	Vengono ignorati gli oggetti di dimensioni (in MB) superiori a quelle specificate nel parametro <dimensione> .
<file configurazione>: definisce il percorso del file di configurazione che contiene le impostazioni di scansione dell'applicazione. Il file di configurazione è in formato testo e contiene l'insieme di parametri da riga di comando per la scansione anti-virus. È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono utilizzati i valori impostati nell'interfaccia dell'applicazione.	
/C:<nome_file>	Vengono utilizzati i valori delle impostazioni specificati nel file di configurazione <nome_file> .
<impostazioni rapporti>: questo parametro determina il formato del rapporto sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.	
/R:<file_rapporti>	In questo file vengono registrati solo gli eventi importanti.
/RA:<file_rapporti>	In questo file vengono registrati tutti gli eventi.
<impostazioni avanzate> : impostazioni che definiscono l'utilizzo delle tecnologie di scansione anti-virus.	
/iChecker=<on off>	Viene abilitato/disabilitato l'utilizzo della tecnologia iChecker.
/iSwift=<on off>	Viene abilitato/disabilitato l'utilizzo della tecnologia iSwift.

Esempi:

- *Avvio di una scansione della memoria, programmi ad esecuzione automatica, caselle di posta, le directory Documenti e Programmi e il file test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\Documenti"
"C:\Programmi" "C:\Downloads\test.exe"
```

- *Sospensione della scansione degli oggetti selezionati e avvio di una scansione completa del computer, al termine della quale continua la scansione sospesa:*

```
avp.com PAUSE Scan_Objects /password=<password>
avp.com START Scan_My_Computer
avp.com RESUME Scan_Objects
```

- *Scansione degli oggetti elencati nel file object2scan.txt mediante il file di configurazione scan_setting.txt per l'operazione. Utilizzo del file di configurazione scan_setting.txt. Al termine della scansione, creare un rapporto per registrare tutti gli eventi:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

File di configurazione di esempio:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

AGGIORNAMENTO DELL'APPLICAZIONE

La sintassi per l'aggiornamento dei moduli e dei database di Kaspersky Anti-Virus dalla riga di comando è la seguente:

```
avp.com UPDATE [<sorgente_aggiornamenti>] [/R[A]:<file_rapporti>] [/C:<nome_file>]
[/APP=<on|off>]
```

Descrizione delle impostazioni:

<sorgente_aggiornamenti>	Server HTTP o FTP o cartella di rete per il download degli aggiornamenti. Il valore del parametro può essere nel formato di un percorso completo di un URL o di una sorgente degli aggiornamenti. Se non viene selezionato un percorso, la sorgente degli aggiornamenti sarà quella delle impostazioni di aggiornamento dell'applicazione.
/R[A]:<file_rapporti>	/R:<file_rapporti> : registra solo eventi importanti nel rapporto. /RA:<report_file> – registra tutti gli eventi nel rapporto. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.
/C:<nome_file>	Percorso del file di configurazione contenente le impostazioni per gli aggiornamenti di Kaspersky Anti-Virus. Un file di configurazione è un file in formato testo che contiene un elenco di parametri da riga di comando per un aggiornamento dell'applicazione. È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono utilizzati i valori delle impostazioni nell'interfaccia dell'applicazione.
/APP=<on off>	Abilita/disabilita gli aggiornamenti dei moduli dell'applicazione.

Esempi:

- ➡ *aggiornamento dei database dell'applicazione e registrazione di tutti gli eventi in un rapporto:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- ➡ *Aggiornamento dei moduli di Kaspersky Anti-Virus mediante i parametri del file di configurazione updateapp.ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

File di configurazione di esempio:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt /app=on
```

ROLLBACK DELL'ULTIMO AGGIORNAMENTO

Sintassi del comando:

```
ROLLBACK [/R[A]:<file_rapporti>] [/password=<password>]
```

Descrizione delle impostazioni:

/R[A]:<file_rapporti>	/R:<file_rapporti> : registra solo eventi importanti nel rapporto. /RA:<report_file> – registra tutti gli eventi nel rapporto. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.
<password>	Password dell'applicazione specificata nell'interfaccia

Questo comando non verrà accettato senza l'immissione di una password.

Esempio:

```
avp.com ROLLBACK /RA:rollback.txt /password=<password>
```

ESPORTAZIONE DELLE IMPOSTAZIONI DI PROTEZIONE

Sintassi del comando:

```
avp.com EXPORT <profilo> <nomefile>
```

Descrizione delle impostazioni:

<profilo>	Componente o attività di cui si esportano le impostazioni. Per <profilo> è possibile utilizzare qualsiasi valore elencato nella sezione della Guida "Gestione dei componenti e delle attività dell'applicazione".
<nomefile>	Percorso nel quale verranno esportate le impostazioni di Kaspersky Anti-Virus. È possibile specificare un percorso assoluto o relativo. Se non viene specificato un formato diverso o se non viene specificato alcun formato, il file di configurazione viene salvato in formato binario (.dat) e può essere utilizzato successivamente per importare le impostazioni in altri computer. Il file di configurazione può inoltre essere salvato come file di testo. A questo scopo, specificare l'estensione .txt nel nome del file. Si noti che non è possibile importare le impostazioni di protezione da un file di testo. Tale file può essere utilizzato solo per specificare le impostazioni principali per il funzionamento di Kaspersky Anti-Virus.

Esempio:

```
avp.com EXPORT c:\settings.dat
```

IMPORTAZIONE DELLE IMPOSTAZIONI DI PROTEZIONE

Sintassi del comando:

```
avp.com IMPORT <nomefile> [/password=<password>]
```

<nomefile>	Percorso del file da cui vengono importate le impostazioni di Kaspersky Anti-Virus. È possibile specificare un percorso assoluto o relativo.
<password>	Password di Kaspersky Anti-Virus specificata nell'interfaccia dell'applicazione. I parametri di protezione possono essere importati solo da un file binario.

Questo comando non verrà accettato senza l'immissione di una password.

Esempio:

```
avp.com IMPORT c:\settings.dat /password=<password>
```

AVVIO DELL'APPLICAZIONE

Sintassi del comando:

```
avp.com
```

ARRESTO DELL'APPLICAZIONE

Sintassi del comando:

```
EXIT /password=<password>
```

<password>	Password dell'applicazione specificata nell'interfaccia
------------	---

Questo comando non verrà accettato senza l'immissione di una password.

CREAZIONE DI UN FILE DI TRACCIA

Se si verificano problemi con Kaspersky Anti-Virus, potrebbe essere necessario creare un file di traccia. I file di traccia sono utili per individuare il problema con maggiore precisione e vengono molto utilizzati dagli esperti dell'Assistenza tecnica.

Sintassi del comando:

```
avp.com TRACE [file] [on|off] [<livello_traccia>]
```

Descrizione delle impostazioni:

[on off]	Abilita/disabilita la creazione del file di traccia
[file]	Inserisce la traccia in un file
<livello_traccia>	Questo valore può essere un numero intero compreso tra 0 (livello minimo, solo messaggi critici) e 700 (livello massimo, tutti i messaggi). Quando si contatta l'Assistenza tecnica, un esperto indica il livello di traccia richiesto. Se non viene specificato alcun valore, si consiglia di impostare il valore su 500.

Si consiglia di creare file di traccia solo per individuare un problema specifico. L'abilitazione regolare delle tracce può rallentare il computer e riempire il disco fisso.

Esempi:

➡ Per disabilitare la creazione del file di traccia:

```
avp.com TRACE file off
```

➡ Per creare un file di traccia da inviare all'Assistenza tecnica con un livello di traccia massimo pari a 500:

```
avp.com TRACE file on 500
```

VISUALIZZAZIONE DELLA GUIDA

Questo comando consente di visualizzare la sintassi della riga di comando dell'applicazione:

```
avp.com [ /? | HELP ]
```

Per visualizzare la Guida per la sintassi di un comando specifico, è possibile utilizzare uno dei comandi seguenti:

```
avp.com <comando> /?
```

```
avp.com HELP <comando>
```

CODICI RESTITUITI DELLA RIGA DI COMANDO

In questa sezione è contenuto un elenco di codici restituiti dalla riga di comando. I codici generali possono essere restituiti da qualsiasi comando dalla riga di comando. I codici restituiti comprendono i codici generali nonché quelli relativi a un tipo specifico di attività.

CODICI RESTITUITI GENERALI	
0	Operazione completata con successo
1	Valore non valido per l'impostazione
2	Errore sconosciuto
3	Errore di completamento dell'attività
4	Attività annullata
CODICI RESTITUITI DALL'ATTIVITÀ DI SCANSIONE ANTI-VIRUS	
101	Tutti gli oggetti pericolosi sono stati elaborati
102	Oggetto pericoloso rilevato

RISOLUZIONE DEI PROBLEMI

Se si verifica un problema durante il funzionamento di Kaspersky Anti-Virus, verificare innanzitutto se nel sistema della Guida o nella Knowledge Base di Kaspersky Lab all'indirizzo <http://support.kaspersky.it> è descritto un metodo per la relativa soluzione. La *Knowledge Base* è una sezione apposita del sito Web del Supporto tecnico di Kaspersky Lab che contiene i consigli per i prodotti Kaspersky Lab e le risposte alle domande più frequenti. Si può provare a trovare una risposta alla propria domanda o una soluzione al proprio problema utilizzando questa risorsa.

➡ *Per accedere alla Knowledge Base:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, cliccare sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** che viene visualizzata, cliccare sul collegamento **Knowledge Base**.

Un'altra risorsa per ottenere informazioni sull'uso dell'applicazione è il forum degli utenti di Kaspersky Lab. Si tratta anche in questo caso di una sezione distinta del sito Web del Supporto tecnico e contiene domande, feedback e richieste degli utenti. È possibile visualizzare gli argomenti principali, lasciare feedback o trovare risposte alle proprie domande.

➡ *Pr aprire il forum degli utenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, cliccare sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** che viene visualizzata, cliccare sul collegamento **Forum degli utenti**.

Se non si trova una soluzione al problema nella Guida, nella Knowledge Base o nel Forum degli utenti, si consiglia di contattare l'assistenza tecnica di Kaspersky Lab.

IN QUESTA SEZIONE:

Creazione di un rapporto sullo stato del sistema	156
Creazione di un file di traccia	156
Invio di file di dati	157
Esecuzione di script AVZ.....	158

CREAZIONE DI UN RAPPORTO SULLO STATO DEL SISTEMA

Per risolvere i problemi dell'utente, gli specialisti di Kaspersky Lab potrebbero aver bisogno di un rapporto sullo stato del sistema. Tale rapporto contiene informazioni dettagliate sui processi in esecuzione, i moduli e i driver caricati, i plug-in di Microsoft Internet Explorer e Microsoft Windows Explorer, le porte aperte, gli oggetti sospetti rilevati e così via.

Quando viene creato un rapporto di stato di sistema, non vengono raccolte informazioni personali dell'utente.

➡ *Per creare un rapporto sullo stato del sistema.*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, cliccare sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** che viene visualizzata, cliccare sul collegamento **Strumenti di assistenza**.
4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, cliccare sul bottone **Crea un rapporto sullo stato del sistema**.

Il rapporto sullo stato del sistema viene creato nei formati *HTML* e *XML* e salvato nell'archivio *sysinfo.zip*. Una volta terminato il processo di raccolta delle informazioni, è possibile visualizzare il rapporto.

➡ *Per visualizzare il rapporto:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, cliccare sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** che viene visualizzata, cliccare sul collegamento **Strumenti di assistenza**.
4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, cliccare sul bottone **Visualizza**.
5. Aprire l'archivio *sysinfo.zip* contenente i file del rapporto.

CREAZIONE DI UN FILE DI TRACCIA

Dopo l'installazione di Kaspersky Anti-Virus, possono verificarsi problemi nel sistema operativo o nel funzionamento di singole applicazioni. La causa più probabile è un conflitto tra Kaspersky Anti-Virus e il software installato nel computer o i driver dei componenti del computer. Per consentire agli specialisti di Kaspersky Lab di risolvere il problema, potrebbe essere necessario creare un file di traccia.

➡ *Per creare il file di traccia:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, cliccare sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** che viene visualizzata, cliccare sul collegamento **Strumenti di assistenza**.
4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, utilizzare l'elenco a discesa nella sezione **Tracciamento** per selezionare il livello di traccia. Tale livello deve essere impostato in base alle indicazioni dello specialista dell'Assistenza tecnica. In assenza di indicazioni da parte dell'Assistenza tecnica, si consiglia di utilizzare il livello di traccia **500**.
5. Per iniziare il processo di creazione di una traccia, scegliere il bottone **Attiva**.
6. Riprodurre la situazione che ha causato il problema.
7. Per arrestare il processo di creazione della traccia, scegliere il bottone **Disattiva**.

È possibile passare al caricamento dei risultati della traccia (vedere la sezione "Invio di file di dati" a pagina [157](#)) a un server di Kaspersky Lab.

INVIO DI FILE DI DATI

Dopo aver creato i file di traccia e il rapporto sullo stato del sistema, sarà necessario inviarli agli esperti del servizio di Assistenza tecnica di Kaspersky Lab.

Per caricare i file di dati sul server dell'Assistenza tecnica, sarà necessario fornire un numero di richiesta. Tale numero è disponibile nella Pagina Personale del sito Web del servizio di Assistenza tecnica, se la richiesta è attiva.

➡ *Per caricare i file di dati sul server del servizio di Assistenza tecnica:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, cliccare sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** che viene visualizzata, cliccare sul collegamento **Strumenti di assistenza**.
4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, sezione **Azioni**, cliccare sul bottone **Invia informazioni sul sistema al servizio di Assistenza**.
5. Nella finestra che viene visualizzata, selezionare le caselle accanto ai file di traccia che si desidera inviare al servizio di Assistenza tecnica e cliccare sul bottone **Invia**.
6. Nella finestra **Inserire il numero della richiesta** visualizzata, specificare il numero assegnato alla richiesta durante il completamento del modulo elettronico nel sito dell'Assistenza tecnica.

I file di traccia selezionati verranno compressi e inviati al server del servizio di Assistenza tecnica.

Se per qualsiasi motivo non si riesce a contattare l'Assistenza tecnica, è possibile salvare i file di dati nel computer.

➡ *Per salvare i file di dati su disco:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, cliccare sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** che viene visualizzata, cliccare sul collegamento **Strumenti di assistenza**.
4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, sezione **Azioni**, cliccare sul bottone **Invia informazioni sul sistema al servizio di Assistenza**.
5. Nella finestra che viene visualizzata, selezionare le caselle accanto ai file di traccia che si desidera inviare al servizio di Assistenza tecnica e cliccare sul bottone **Invia**.
6. Nella finestra **Inserire il numero della richiesta** visualizzata, cliccare sul bottone **Annulla** e confermare il salvataggio dei file sul disco.
7. Nella finestra che viene visualizzata specificare il nome dell'archivio.

Successivamente sarà possibile inviare i file salvati all'Assistenza tecnica utilizzando la Pagina personale (<https://support.kaspersky.com/ru/personalcabinet?LANG=it>).

ESECUZIONE DI SCRIPT AVZ

Gli esperti di Kaspersky Lab analizzeranno il problema rilevato dall'utente utilizzando i file di traccia e il rapporto sullo stato del sistema ricevuti. Il risultato dell'analisi è una sequenza di azioni mirate a eliminare i problemi rilevati. L'elenco di azioni può essere piuttosto lungo.

Per semplificare la procedura, si utilizzano script AVZ. Uno script AVZ è un insieme di istruzioni che consentono di modificare le chiavi di registro, mettere in quarantena i file, ricercare le classi di file con la possibilità di mettere in quarantena i file a esse correlati, bloccare gli intercettori UserMode e KernelMode e così via.

Per eseguire gli script, l'applicazione include una *procedura guidata di esecuzione di script AVZ*. La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Indietro** e **Avanti**. Per chiudere la procedura guidata al completamento, utilizzare il bottone **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il bottone **Annulla**.

Non è consigliabile modificare il testo dello script AVZ ricevuto dagli esperti di Kaspersky Lab. Se il problema si verifica durante l'esecuzione dello script, contattare il servizio di Assistenza tecnica.

➡ Per avviare la procedura guidata:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, cliccare sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** visualizzata, cliccare sul collegamento **Strumenti di assistenza** nella parte inferiore della finestra.
4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, cliccare sul bottone **Esegui uno script con AVZ**.

Se lo script viene eseguito correttamente, la procedura guidata si chiude. Se si verifica un errore durante l'esecuzione dello script, viene visualizzato un messaggio di errore corrispondente nella procedura guidata.

INFORMATIVA SULLA RACCOLTA DATI PER KASPERSKY SECURITY NETWORK

A. INTRODUZIONE

Leggere attentamente il presente documento. In quanto contiene informazioni utili per poter continuare a utilizzare i servizi o il software messi a disposizione da Kaspersky Lab. L'uso prolungato dei suddetti servizi e del software comporta l'accettazione delle condizioni illustrate nella presente informativa sulla raccolta dei dati. Kaspersky Lab si riserva il diritto di modificare l'Informativa sulla raccolta dei dati in qualsiasi momento e di comunicare gli eventuali cambiamenti in questa pagina. La data di revisione riportata in basso consente di determinare se sono state apportate modifiche dall'ultima consultazione del documento. L'uso prolungato dei servizi Kaspersky Lab a seguito della pubblicazione degli aggiornamenti dell'Informativa sulla raccolta dei dati costituisce implicita accettazione delle modifiche apportate.

L'obiettivo della presente Informativa sulla raccolta dei dati creata da Kaspersky Lab e relativi consociati (collettivamente definiti "Kaspersky Lab") è di informare l'utente sulle pratiche di raccolta e diffusione dei dati adottate per i prodotti Kaspersky Anti-Virus e Kaspersky Internet Security.

Gli impegni assunti da Kaspersky Lab

L'impegno costante di Kaspersky Lab nell'offerta di un servizio qualitativamente elevato a tutti i clienti si concentra soprattutto sulle procedure di raccolta dei dati. Per rispondere a tutte le domande e fugare gli eventuali dubbi che potrebbero sorgere relativamente alle procedure adottate dal servizio Kaspersky Security Network per la raccolta dei dati, è stata creata la presente "Informativa sulla raccolta dei dati" (definita anche semplicemente "Informativa").

In questo documento vengono descritte, in termini generali e con numerosi dettagli tecnici, tutte le precauzioni adottate per garantire un corretto uso dei dati raccolti. L'organizzazione dei contenuti per procedure e aree principali facilita una rapida identificazione e lettura delle informazioni desiderate. L'obiettivo primario di Kaspersky Lab è di soddisfare le esigenze e le aspettative dei propri clienti e la protezione dei dati raccolti rappresenta uno degli impegni prioritari.

La raccolta dei dati e delle informazioni viene effettuata direttamente da Kaspersky Lab. Per domande o dubbi sul contenuto dell'Informativa, inviare un messaggio e-mail all'indirizzo support@kaspersky.com.

Kaspersky Security Network

Il servizio Kaspersky Security Network consente agli utenti dei prodotti per la protezione Kaspersky Lab di tutto il mondo di identificare più facilmente i rischi sempre più numerosi e di ridurre il tempo necessario per garantire la protezione del computer. Per identificare le nuove minacce e le relative fonti e migliorare la protezione dell'utente e le funzionalità del prodotto, Kaspersky Security Network raccoglie dati selezionati sulla protezione e sull'applicazione e li invia a Kaspersky Lab per l'analisi. Tali informazioni non contengono dati che consentono l'identificazione personale dell'utente e vengono utilizzate da Kaspersky Lab al solo scopo di migliorare i prodotti per la protezione e perfezionare le soluzioni sviluppate per contrastare minacce e virus. Qualora si verifichi una trasmissione accidentale di dati personali dell'utente, Kaspersky Lab adotterà tutte le misure di protezione necessarie, in conformità con quanto sancito nella presente Informativa.

Partecipando a Kaspersky Security Network, tutti gli utenti dei prodotti per la protezione Kaspersky Lab in tutto il mondo contribuiscono in modo significativo al miglioramento della sicurezza di Internet.

Aspetti legali

Kaspersky Security Network può essere soggetto a diverse giurisdizioni, inclusa quella degli Stati Uniti d'America, a seconda del paese in cui vengono utilizzati i servizi. Kaspersky Lab divulgherà le informazioni personali senza previa notifica se richiesto per legge o nella ferma convinzione che tale azione sia necessaria per approfondire la natura di determinate attività dannose o proteggere dalle stesse ospiti, visitatori, associati Kaspersky Lab o altri utenti. Come descritto in precedenza, la legislazione relativa ai dati e alle informazioni raccolte da Kaspersky Security Network può variare da paese a paese. Ad esempio, alcune informazioni che consentono l'identificazione personale raccolte nell'Unione Europea e negli Stati membri sono soggette alle Direttive relative a dati personali, privacy e comunicazioni elettroniche, incluse, a titolo esemplificativo, la Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativa all'elaborazione dei dati personali e alla protezione della privacy nel settore delle comunicazioni elettroniche.

e la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 sulla protezione degli individui con riferimento all'elaborazione dei dati personali e alla libera circolazione di tali dati e alla successiva legislazione adottata negli Stati membri dell'Unione Europea, la decisione della Commissione Europea 497/2001/CE sulle clausole contrattuali-tipo (trasferimento di dati personali verso paesi terzi) e la legislazione successiva adottata negli Stati membri.

Kaspersky Security Network avviserà gli utenti interessati, durante la raccolta iniziale delle informazioni appena descritte, dell'eventuale condivisione di tali informazioni, soprattutto se è previsto un impiego per uno sviluppo commerciale e offrirà a tali utenti Internet la possibilità di accettare (negli Stati membri dell'Unione Europea e in altri paesi che richiedono la procedura di opt-in) o di rinunciare (per tutti gli altri paesi) online all'uso commerciale di tali dati e/o la trasmissione degli stessi a terze parti.

Kaspersky Lab potrebbe essere obbligata per legge o da autorità giudiziarie a fornire alcune informazioni che consentono l'identificazione personale agli enti governativi appropriati. Nei casi sopra citati, tali informazioni verranno fornite previa ricezione della documentazione appropriata. Kaspersky Lab potrebbe anche essere tenuta per legge a fornire informazioni per proteggere la proprietà oltre che il benessere e la sicurezza degli individui.

Le dichiarazioni alle autorità degli Stati membri per la protezione dei dati personali verranno effettuate in base alla legislazione successiva degli Stati membri dell'Unione Europea in vigore. Le informazioni su tali dichiarazioni saranno accessibili nei servizi Kaspersky Security Network.

B. INFORMAZIONI RACCOLTE

Tipologie di dati raccolti

Gli utenti hanno il diritto di concedere i dati in base alla presente informativa. Il servizio Kaspersky Security Network raccoglie e invia a Kaspersky Lab due categorie di dati sui rischi di protezione potenziali che minacciano il computer, ovvero:

- **Dati principali:**
 - informazioni sul software e l'hardware installato sul computer, compreso il sistema operativo ed i service pack installati, gli oggetti kernel, i driver, i servizi, le estensioni di Internet Explorer, le estensioni del sistema di stampa, le estensioni di Esplora risorse, i programmi scaricati, elementi di impostazione attivi, gli applet del pannello di controllo, le voci del file Hosts e del registro, gli indirizzi IP, i tipi di browser, i client di posta elettronica ed il numero di versione dei prodotti di Kaspersky Lab, che sono di solito informazioni non personalmente identificabili.
 - una ID univoca generata dal prodotto di Kaspersky Lab per identificare le singole macchine senza identificare l'utente, che non contiene informazioni personali.
 - informazioni sullo stato della protezione anti-virus del computer, e dati su qualsiasi file o attività per cui esista il sospetto di programma nocivo (es. nome virus, data/ora di rilevamento, nomi/percorsi e dimensione dei file infetti, IP e porta dell'attacco di rete, nome dell'applicazione sospettata di essere nociva). Tenere presente che i dati raccolti appena descritti non contengono informazioni che consentono l'identificazione personale.
- **Dati estesi:**
 - informazioni sulle applicazioni firmate digitalmente scaricate dell'utente (URL, dimensione file, nome firmatario);
 - informazioni sulle applicazioni eseguibili (dimensioni, attributi, data di creazione, informazioni sulle intestazioni PE, regione, nome, ubicazione e utilità di compressione utilizzata).
- **File e/o loro parti.** Il servizio Kaspersky Security Network può raccogliere e inviare file interi e/o loro parti a Kaspersky Lab per sottoporli a un'ulteriore analisi. I trasferimenti di file e/o loro parti vengono eseguiti solo se l'Informativa sulla raccolta dei dati di Kaspersky Lab è stata accettata dall'utente.

Protezione della trasmissione e dell'archiviazione dei dati

Kaspersky Lab garantisce la protezione delle informazioni che raccoglie. Le informazioni raccolte vengono archiviate in server con accesso limitato e controllato. Kaspersky Lab gestisce reti di dati protette da firewall standard del settore e sistemi con password di protezione. Utilizza inoltre una vasta gamma di procedure e tecnologie di protezione delle informazioni raccolte da minacce come l'uso, la divulgazione o accessi non autorizzati. I criteri di protezione vengono periodicamente aggiornati e migliorati se necessario e solo le persone autorizzate possono accedere ai dati raccolti. Kaspersky Lab adotta tutte le misure necessarie per garantire che le informazioni vengano gestite all'insegna della protezione e in conformità con la presente Informativa. Sfortunatamente, nessuna trasmissione di dati può essere considerata sicura al 100%. Di conseguenza, sebbene il nostro impegno nella protezione dei dati sia molto forte, non è possibile garantire la protezione completa dei dati trasmessi dall'utente o derivanti dai prodotti o dai servizi, incluso il programma Kaspersky Security Network, e tutti questi servizi vengono utilizzati a rischio dell'utente.

I dati raccolti possono essere trasferiti nei server di Kaspersky Lab e Kaspersky Lab ha adottato tutte le precauzioni necessarie per garantire che le informazioni raccolte, se trasferite, ricevano un livello appropriato di protezione. I dati raccolti vengono considerati informazioni riservate e in quanto tali sono soggetti alle procedure di sicurezza e ai criteri aziendali relativi alla protezione e all'uso di informazioni riservate. Una volta giunti presso Kaspersky Lab, i dati raccolti vengono archiviati in un server con caratteristiche di sicurezza fisiche ed elettroniche standard del settore, incluso l'utilizzo di procedure di accesso/password e firewall elettronici progettati per bloccare l'accesso non autorizzato dall'esterno di Kaspersky Lab. I dati raccolti da Kaspersky Security Network descritti nella presente Informativa vengono elaborati e archiviati negli Stati Uniti e in altre giurisdizioni e in altri paesi in cui Kaspersky Lab ha interessi commerciali. Tutti i dipendenti Kaspersky Lab sono a conoscenza dei criteri di protezione. I dati forniti dagli utenti sono accessibili solo ai dipendenti che ne prendono visione per svolgere il proprio lavoro. Tutti i dati archiviati non verranno associati a informazioni che consentono l'identificazione personale. Kaspersky Lab non combina i dati archiviati da Kaspersky Security Network ad altri dati, elenchi di contatti o informazioni sull'abbonamento raccolti da Kaspersky Lab a scopo promozionale o per altre finalità.

C. USO DEI DATI RACCOLTI*Uso dei dati personali*

Kaspersky Lab raccoglie i dati per analizzare e identificare la fonte dei rischi potenziali della protezione e per migliorare la capacità dei prodotti di Kaspersky Lab di rilevare comportamenti dannosi, siti Web fraudolenti, crimeware e altri tipi di minacce alla protezione di Internet per offrire il miglior livello possibile di protezione ai clienti Kaspersky Lab nel futuro.

Diffusione delle informazioni a terze parti

Kaspersky Lab può divulgare le informazioni raccolte per legge o in risposta a una citazione in giudizio o a un altro processo legale o nella ferma convinzione che tale azione sia necessaria per ottemperare a un obbligo di legge, rispondere a una citazione in giudizio o a un altro processo legale o richiesta governativa. Kaspersky Lab può inoltre diffondere informazioni che consentono l'identificazione personale nei casi in cui ritenga che tali informazioni siano necessarie per identificare, contattare o avviare un'azione legale contro chiunque violi tale Informativa, i termini degli accordi con la società o per proteggere la sicurezza degli utenti e gli accordi pubblici o di riservatezza con determinate terze parti che collaborano con Kaspersky nello sviluppo e nella gestione di Kaspersky Security Network. Per favorire la consapevolezza, il rilevamento e la prevenzione dei rischi della protezione di Internet, Kaspersky Lab può condividere determinate informazioni con organizzazioni di ricerca e altri fornitori di software per la protezione. Può altresì utilizzare le statistiche derivate dalle informazioni raccolte per registrare e pubblicare rapporti sulle tendenze dei rischi della protezione.

Opzioni disponibili all'utente

La partecipazione al programma Kaspersky Security Network è facoltativa. È possibile attivare e disattivare il servizio Kaspersky Security Network in qualsiasi momento modificando le impostazioni Feedback nella pagina delle opzioni del prodotto Kaspersky Lab in uso. È tuttavia importante ricordare che se si sceglie di disattivare il servizio Kaspersky Security Network, potrebbe non essere possibile offrire alcuni dei servizi dipendenti dalla raccolta dei dati. Al termine del periodo di validità del prodotto Kaspersky Lab, alcune funzioni del software Kaspersky Lab potrebbero essere ancora attive, ma le informazioni non verranno più inviate automaticamente a Kaspersky Lab.

Kaspersky Lab si riserva anche il diritto di inviare messaggi di avviso occasionali agli utenti per informarli di modifiche specifiche che potrebbero influire sulla propria capacità di utilizzare i servizi per i quali è stato sottoscritto un abbonamento. Si riserva inoltre il diritto di contattare gli utenti se obbligata nell'ambito di un procedimento legale o se si è verificata una violazione di un accordo di licenza, garanzia o acquisto.

Kaspersky Lab mantiene tali diritti in quanto in casi limitati potrebbe essere necessario contattare l'utente per un obbligo di legge o per discutere di questioni importanti per l'utente stesso. Tali diritti non consentono di contattare l'utente per la promozione e la vendita di prodotti nuovi o esistenti in assenza di un consenso esplicito e l'invio di questi tipi di comunicazioni è raro.

D. RACCOLTA DEI DATI – DOMANDE E RECLAMI CORRELATI

Kaspersky Lab gestisce ed esamina con il massimo rispetto e la più grande attenzione le perplessità dei clienti sulla raccolta dei dati. Per segnalare un caso di mancata conformità alla presente Informativa relativamente al trattamento dei propri dati o per porre domande sulla gestione dei dati riservati, è possibile scrivere all'indirizzo e-mail: support@kaspersky.com.

Spiegare la natura della richiesta utilizzando il maggior numero di dettagli possibile. Alla domanda verrà fornita una risposta in tempi brevi.

La fornitura delle informazioni è facoltativa. L'opzione relativa alla raccolta dei dati può essere disattivata dall'utente in qualsiasi momento nella sezione "Feedback" della pagina "Impostazioni" del prodotto Kaspersky in uso.

© 1997-2009 Kaspersky Lab ZAO. Tutti i diritti riservati.

UTILIZZO DI CODICE DI TERZE PARTI

Il codice di terze parti è stato utilizzato durante la fase di sviluppo di Kaspersky Anti-Virus.

IN QUESTA SEZIONE:

Libreria Crypto C (libreria di software per la protezione dei dati)	164
Libreria Fastscript 1.9	164
Libreria libnkfm 7.4.7.7	164
Libreria del parser Bison GNU	165
Libreria AGG 2.4	165
Libreria OpenSSL 0.9.8d	166
Libreria Gecko SDK 1.8	167
Libreria Zlib 1.2	167
Libreria libpng 1.2.8, 1.2.29	167
Libreria Libnkfm 2.0.5	167
Libreria Expat 1.2, 2.0.1	168
Libreria Info-ZIP 5.51	168
Libreria Windows Installer XML (WiX) 2.0	169
Libreria Passthru	171
Libreria Filter	171
Libreria Netcfg	172
Libreria Pcre 3.0	172
Libreria RFC1321-based (RSA-free) MD5	172
Libreria Windows Template (WTL 7.5)	172
Libreria Libjpeg 6b	175
Libreria Libungif 3.0	176
Libreria Libxdr	176
Libreria Tiniconv - 1.0.0	177
Libreria Bzip2/libbzip2 1.0.5	182
Libreria Libspf2-1.2.9	182
Libreria Protocol Buffer	183

LIBRERIA CRYPTO C (LIBRERIA DI SOFTWARE PER LA PROTEZIONE DEI DATI)

Per creare e controllare le firme digitali viene utilizzata la libreria di software per la protezione dei dati Crypto C, sviluppata da "CryptoEX", <http://www.cryptoex.ru>.

LIBRERIA FASTSCRIPT 1.9

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria FastScript. Copyright © Fast Reports Inc. All rights reserved.

LIBRERIA LIBNKFM 7.4.7.7

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria PCRE 7.4 copyright © 1997-2008 University of Cambridge in base ai termini della licenza BSD.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" license, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBRERIA DEL PARSER BISON GNU

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria dello scheletro del parser Bison 2.3 copyright © GNU Project <http://ftp.gnu.org/gnu/bison/> in base a un'eccezione speciale.

As a special exception, you may create a larger work that contains part or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

LIBRERIA AGG 2.4

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria AGG (Anti-Grain Geometry) 2.4 copyright © 2002-2005 Maxim Shemanarev. All rights reserved, su licenza BSD modificata.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

LIBRERIA OPENSSL 0.9.8d

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria OpenSSL 0.9.8d copyright © 1998-2007 The OpenSSL Project. All rights reserved, su licenza OpenSSL License e Original SSLeay License (<http://www.openssl.org/>).

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

LIBRERIA GECKO SDK 1.8

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Gecko SDK 1.8 Copyright © Mozilla Foundation. All rights reserved, su licenza MPL 1.1 (<http://www.mozilla.org/MPL/MPL-1.1.html>). Sito Web e collegamento del pacchetto di distribuzione: http://developer.mozilla.org/en/docs/Gecko_SDK.

LIBRERIA ZLIB 1.2

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria zlib 1.2 copyright © 1995-2005 Jean-loup Gailly and Mark Adler. All rights reserved, su licenza zlib/libpng.

LIBRERIA LIBPNG 1.2.8, 1.2.29

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libpng 1.2.8, 1.2.29 copyright © 2004, 2006-2008 Glenn Randers-Pehrson. All rights reserved, su licenza zlib/libpng.

LIBRERIA LIBNKFM 2.0.5

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libnkfm 2.0.5 Copyright (c) KUBO Takehiro. All rights reserved.

LIBRERIA EXPAT 1.2, 2.0.1

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Expat 1.2, 2.0.1 Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd. All rights reserved. Utilizzo in base alle condizioni seguenti:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBRERIA INFO-ZIP 5.51

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Info-ZIP 5.51 Copyright (c) 1990-2007. All rights reserved, su licenza Info-ZIP.

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip", "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.
4. Info-ZIP retains the right to use the names "Info-ZIP", "Zip", "UnZip", "UnZipSFX", "WiZ", "Pocket UnZip", "Pocket Zip", and "MacZip" for its own source and binary releases.

LIBRERIA WINDOWS INSTALLER XML (WiX) 2.0

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Windows Installer XML (WiX) 2.0 Copyright (c) Microsoft Corporation. All rights reserved, su licenza CPL 1.0 (<http://sourceforge.net/projects/wix/>).

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:
 - i) changes to the Program, and
 - ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

- a) it complies with the terms and conditions of this Agreement; and
- b) its license agreement:
 - i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;
 - ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;
 - iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and
 - iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

- a) it must be made available under this Agreement; and
- b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

LIBRERIA PASSTHRU

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Ndis Intermediate Miniport driver sample Copyright (c) 1992-2000 Microsoft Corporation. All rights reserved.

LIBRERIA FILTER

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Ndis Sample NDIS Lightweight filter driver Copyright (c) 2004-2005 Microsoft Corporation. All rights reserved.

LIBRERIA NETCFG

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Network Configuration Sample Copyright (c) 1997 Microsoft Corporation. All rights reserved.

LIBRERIA PCRE 3.0

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria pcre 3.0 copyright © 1997-1999 University of Cambridge in base alla PCRE LICENSE. All rights reserved.

LIBRERIA RFC1321-BASED (RSA-FREE) MD5

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria RFC1321-based (RSA-free) MD5. Copyright (c) 1999, 2002 Aladdin Enterprises. All rights reserved. Distribuita su licenza zlib/libpng.

LIBRERIA WINDOWS TEMPLATE (WTL 7.5)

Windows Template Library 7.5 Copyright (c) 2005 Microsoft Corporation was used during application development. All rights reserved, su licenza Common Public License 1.0, <http://sourceforge.net/projects/wtl/>.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:
 - i) changes to the Program, and
 - ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

LIBRERIA LIBJPEG 6B

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libjpeg 6b. Copyright (c) 1991-1998, Thomas G. Lane. All Rights. L'utilizzo si basa sulle condizioni seguenti:

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBRERIA LIBUNGIF 3.0

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libungif 3.0. Copyright (c) 1997 Eric S. Raymond. L'utilizzo si basa sulle condizioni seguenti:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBRERIA LIBXDR

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libxdr copyright © Sun Microsystems, Inc. L'utilizzo si basa sulle condizioni seguenti:

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

LIBRERIA TINICONV - 1.0.0

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria tiniconv – 1.0.0. Copyright (C) Free Software Foundation, Inc. author Roman Rybalko (<http://sourceforge.net/projects/tiniconv/>) under GNU LGPL 2,1 license (<http://www.gnu.org/>).

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

LIBRERIA BZIP2/LIBBZIP2 1.0.5

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria bzip2/libbzip2 1.0.5. Copyright (C) 1996-2007 Julian R Seward. All rights reserved. L'utilizzo si basa sulle condizioni seguenti:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org

LIBRERIA LIBSPF2-1.2.9

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libspf2-2/1/09. Copyright 2005 by Shevek and Wayne Schlitt. All rights reserved. Utilizzo in base alle condizioni della licenza The two-clause BSD:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBRERIA PROTOCOL BUFFER

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Protocol Buffer. Copyright 2008, Google Inc. All rights reserved. Distribuita in base alle condizioni della licenza New BSD.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

GLOSSARIO

Elenco di maschere e indirizzi di risorse Web, di cui l'utente considera attendibile il contenuto. L'applicazione Kaspersky Lab non sottopone a scansione le pagine Web, corrispondenti ad alcune voci dell'elenco, per verificare la presenza di oggetti dannosi.

AGGIORNAMENTI DEL DATABASE

Una delle funzioni eseguite da un'applicazione Kaspersky Lab che consente di tenere sempre aggiornata la protezione. I database vengono scaricati dai server degli aggiornamenti di Kaspersky Lab nel computer e collegati automaticamente all'applicazione.

AGGIORNAMENTI DISPONIBILI

Gruppo di aggiornamenti per i moduli dell'applicazione Kaspersky Lab, inclusi gli aggiornamenti critici accumulati in un periodo di tempo e le modifiche apportate all'architettura dell'applicazione.

AGGIORNAMENTI URGENTI

Aggiornamenti critici ai moduli dell'applicazione Kaspersky Lab.

AGGIORNAMENTO

Procedura di sostituzione/aggiunta di nuovi file (database o moduli dell'applicazione) recuperati dai server degli aggiornamenti di Kaspersky Lab.

ANALIZZATORE EURISTICO

Tecnologia di rilevamento delle minacce che non possono essere identificate dai database Anti-virus. Consente di rilevare gli oggetti sospettati di essere stati colpiti da un virus sconosciuto o da una variante nuova di virus noti.

L'utilizzo dell'analizzatore euristico consente di rilevare fino al 92% delle minacce. Questo meccanismo è estremamente efficace e determina falsi positivi molto raramente.

I file rilevati dall'analizzatore euristico sono considerati sospetti.

APPLICAZIONE NON COMPATIBILE

Applicazione anti-virus di uno sviluppatore di terze parti o applicazione Kaspersky Lab che non supporta la gestione attraverso Kaspersky Administration Kit.

ARCHIVIO

File "contenenti" uno o diversi altri oggetti che possono anche essere archivi.

ATTACCO DI VIRUS

Serie di attacchi intenzionali per infettare un computer con un virus.

ATTIVAZIONE DELL'APPLICAZIONE

La procedura di attivazione dell'applicazione consiste nell'immissione di un codice di attivazione e nell'ottenimento di una chiave che consentirà all'applicazione di determinare se l'utente dispone di diritti sufficienti per utilizzarla e di conoscere la data di scadenza della licenza.

ATTIVITÀ

Le funzioni eseguite dall'applicazione di Kaspersky Lab vengono implementate come attività, ad esempio: **Protezione in tempo reale**, **Scansione Completa del computer**, **Aggiornamento del database**.

BLACKLIST DEI FILE CHIAVE

Database contenente informazioni sui file chiave Kaspersky Lab inseriti nella blacklist i cui proprietari hanno violato i termini del Contratto di licenza e informazioni sui file di chiave emessi ma per qualche motivo non venduti o sostituiti. Un file della blacklist è necessario per il funzionamento delle applicazioni di Kaspersky Lab. Il contenuto del file viene aggiornato insieme ai database.

BLOCCO DELL'OGGETTO

Negazione dell'accesso a un oggetto da applicazioni esterne. Un oggetto bloccato non può essere letto, eseguito, modificato o eliminato.

CERTIFICATO DEL SERVER DI AMMINISTRAZIONE

Certificato che consente di autenticare il server di amministrazione quando viene connesso alla console di amministrazione e durante lo scambio di dati con i computer degli utenti. Il certificato del server di amministrazione viene creato durante l'installazione del server di amministrazione e viene memorizzato nella sottocartella **Cert** della cartella di installazione dell'applicazione.

CONTATORE DEGLI ATTACCHI D VIRUS

Modello in base al quale viene generata una notifica di minaccia di attacco di virus. Il contatore include una combinazione di impostazioni che determinano la soglia dell'attività del virus, la modalità di diffusione e il testo nei messaggi da inviare.

COPIA DI BACKUP

Creazione di una copia di backup di un file prima di qualsiasi elaborazione; la copia viene archiviata nella memoria di backup e consente di ripristinare il file in seguito, ad esempio per eseguire una scansione con database aggiornati.

DATABASE

Database creati dagli esperti di Kaspersky Lab contenenti una descrizione dettagliata di tutte le minacce alla sicurezza del computer attualmente esistenti nonché dei metodi per rilevarle ed eliminarle. I database vengono costantemente aggiornati da Kaspersky Lab al presentarsi di nuove minacce. Per ottenere una migliore qualità di rilevamento delle minacce, è consigliabile copiare regolarmente i database dai server di aggiornamento di Kaspersky Lab.

DATABASE DELLA POSTA

Database contenenti messaggi di posta elettronica in un formato speciale salvati nel computer. Ogni messaggio di posta in entrata e in uscita viene inserito nel database della posta dopo essere stato ricevuto/inviato. I database vengono esaminati durante la scansione completa del computer.

I messaggi in entrata e in uscita vengono analizzati per cercare eventuali virus in tempo reale al momento dell'invio e della ricezione, se la protezione in tempo reale è abilitata.

DATABASE DI INDIRIZZI WEB DI PHISHING

Elenco di indirizzi Web, definiti come phishing dagli specialisti di Kaspersky Lab. Il database viene aggiornato regolarmente e fa parte dell'applicazione Kaspersky Lab.

DATABASE DI INDIRIZZI WEB SOSPETTI

Elenco di indirizzi Web, il cui contenuto può essere considerato come potenzialmente pericoloso. L'elenco viene creato dagli specialisti di Kaspersky Lab, regolarmente aggiornato e incluso nel pacchetto dell'applicazione Kaspersky Lab.

DISINFEZIONE DEGLI OGGETTI

Metodo utilizzato per elaborare gli oggetti infetti che consente di recuperare completamente o parzialmente i dati; in caso contrario l'oggetto viene considerato impossibile da disinfettare. La disinfezione degli oggetti viene eseguita in base alle voci dei database. Durante la disinfezione è possibile che parte dei dati venga persa.

DISINFEZIONE DEGLI OGGETTI AL RIAVVIO

Metodo di elaborazione degli oggetti infetti utilizzati da altre applicazioni al momento della disinfezione. Consiste nel creare una copia dell'oggetto infetto, disinfettare la copia creata e sostituire l'oggetto infetto originale con la copia disinfettata dopo il riavvio successivo del sistema.

DNS (DOMAIN NAME SERVICE)

Sistema distribuito per la conversione del nome di un host (un computer o un altro dispositivo di rete) in un indirizzo IP. Il DNS funziona in reti TCP/IP. In particolare può anche memorizzare ed elaborare richieste inverse, determinando il nome di un host in base al relativo indirizzo IP (record PTR). La risoluzione dei nomi DNS viene in genere eseguita da applicazioni di rete, non dagli utenti.

ELENCO DI INDIRIZZI WEB ESAMINATI

Elenco di maschere e indirizzi di risorse Web, esaminati obbligatoriamente alla ricerca di oggetti dannosi da parte dell'applicazione Kaspersky Lab.

ELIMINAZIONE DI UN OGGETTO

Metodo di elaborazione dell'oggetto che implica la sua eliminazione fisica dalla posizione originaria (disco rigido, cartella, risorsa di rete). Si consiglia di applicare questo metodo agli oggetti pericolosi che, per qualsiasi ragione, non possono essere disinfettati.

ESCLUSIONE

Per esclusione si intende un oggetto escluso dalla scansione da parte dell'applicazione Kaspersky Lab. È possibile escludere dalla scansione determinati formati di file, utilizzare una maschera file o escludere una determinata area, ad esempio una cartella o un programma, processi di programma o oggetti in base alla classificazione del tipo di minaccia nell'Enciclopedia dei Virus. A ogni attività può essere assegnato un insieme di esclusioni.

FILE CHIAVE

File con estensione **key**, che rappresenta la "chiave" personale che consente di utilizzare l'applicazione Kaspersky Lab. Un file chiave viene incluso nel prodotto acquistato presso i distributori Kaspersky Lab o inviato tramite posta elettronica se l'acquisto avviene online.

FILE COMPRESSO

File di archivio contenente un programma di decompressione e istruzioni per l'esecuzione per il sistema operativo.

FLUSSI NTFS ALTERNATIVI

Flussi di dati NTFS (flussi di dati alternativi) destinati a contenere attributi aggiuntivi o informazioni sul file.

Ogni file nel file system NTFS è un insieme di flussi. Uno di essi include il contenuto del file che sarà possibile visualizzare dopo aver aperto il file, altri flussi (definiti alternativi) sono destinati a contenere meta informazioni e garantire, ad esempio, la compatibilità NTFS con altri sistemi, come un file system precedente di Macintosh definito HFS (Hierarchical File System). I flussi possono essere creati, eliminati, memorizzati, rinominati e persino eseguiti come un processo.

I flussi alternativi possono essere utilizzati dagli utenti malintenzionati per trasferire dati in segreto o per rubarli da un computer.

GATEWAY CON DOPPIO-HOME

Computer fornito di due schede di rete, ciascuna delle quali collegata a reti diverse, che trasferisce i dati da una rete all'altra.

IMPOSTAZIONI ATTIVITÀ

Impostazioni dell'applicazione specifiche per ogni tipo di attività.

IMPOSTAZIONI DELL'APPLICAZIONE

Impostazioni dell'applicazione comuni a tutti i tipi di attività, che regolano il funzionamento dell'applicazione nel suo complesso, ad esempio le impostazioni relative alle prestazioni, ai rapporti e alla memoria di backup.

INSTALLAZIONE CON UNO SCENARIO DI AVVIO

Metodo di installazione remota delle applicazioni Kaspersky Lab che consente di assegnare l'avvio dell'attività di installazione remota a un singolo account utente o a più account utente. La registrazione di un utente in un dominio porta a un tentativo di installazione dell'applicazione nel computer client in cui l'utente è registrato. Questo metodo è consigliato per l'installazione delle applicazioni in computer che eseguono i sistemi operativi Microsoft Windows 98/Me.

INTERCETTATORE

Subcomponente dell'applicazione responsabile della scansione di tipi specifici di messaggi di posta. Il set di intercettori specifico dell'installazione dipende dal ruolo o dalla combinazione di ruoli per i quali l'applicazione è stata distribuita.

INTESTAZIONE

Informazioni all'inizio di un file o di un messaggio, composti da dati di basso livello sullo stato e l'elaborazione del file (o del messaggio). In particolare, l'intestazione del messaggio di posta elettronica contiene dati come le informazioni sul mittente e il destinatario, nonché la data.

IP (INTERNET PROTOCOL)

Il protocollo base per Internet, utilizzato sin dai tempi del suo primo sviluppo nel 1974. Esegue operazioni elementari nella trasmissione di dati da un computer all'altro e rappresenta la base per protocolli di livello superiore come TCP e UDP. Gestisce la connessione e l'elaborazione degli errori. Il ricorso a tecnologie come il NAT e il mascheramento consente di nascondere un gran numero di reti private attraverso un numero limitato di indirizzi IP (o persino un indirizzo). In questo modo diventa possibile gestire le richieste della rete Internet in costante espansione attraverso uno spazio degli indirizzi IPv4 relativamente limitato.

LICENZA AGGIUNTIVA

Licenza aggiunta per consentire il funzionamento dell'applicazione Kaspersky Lab ma non attivata. La licenza aggiuntiva viene attivata alla scadenza della licenza attiva.

LICENZA ATTIVA

La licenza attualmente utilizzata per il funzionamento di un'applicazione Kaspersky Lab. La licenza definisce la data di scadenza della funzionalità completa e i criteri della licenza relativi all'applicazione. È consentita una sola licenza con lo stato attivo.

LIVELLO CONSIGLIATO

Livello di protezione basato sulle impostazioni dell'applicazione consigliate dagli esperti di Kaspersky Lab per offrire il livello ottimale di protezione per il computer. Il livello viene impostato per essere utilizzato per impostazione predefinita.

LIVELLO DI GRAVITÀ DELL'EVENTO

Descrizione dell'evento, registrato durante il funzionamento dell'applicazione Kaspersky Lab. Esistono quattro livelli di gravità:

- **Eventi critici.**
- **Errori funzionali.**
- **Attenzione!**
- **Messaggio informativo.**

Eventi dello stesso tipo possono avere livelli di gravità diversi, in base alla situazione in cui si sono verificati.

LIVELLO DI PROTEZIONE

Il livello di protezione viene definito come una configurazione del componente predeterminata.

MASCHERA FILE

Rappresentazione di un'estensione e di un nome file tramite caratteri jolly. I due caratteri jolly standard utilizzati nelle maschere di file sono * e ?, dove * rappresenta qualsiasi numero di caratteri e ? indica qualsiasi carattere singolo. Utilizzando questi caratteri jolly, è possibile rappresentare qualsiasi file. Notare che il nome e l'estensione sono sempre separati da un punto.

MEMORIA DI BACKUP

Memoria speciale destinata al salvataggio delle copie di backup di oggetti creati prima della prima disinfezione o eliminazione.

MODELLO DI NOTIFICA

Modello in base al quale viene generata una notifica di oggetti infetti rilevati dalla scansione. Il modello di notifica include una combinazione di impostazioni che regolano la modalità di notifica, la modalità di diffusione e il testo dei messaggi da inviare.

MODULI DELL'APPLICAZIONE

File inclusi nel pacchetto di installazione di Kaspersky Lab responsabile dell'esecuzione delle attività principali. Un determinato modulo eseguibile corrisponde a ogni tipo di attività eseguita dall'applicazione (protezione in tempo reale, scansione a richiesta, aggiornamenti). Attraverso l'esecuzione di una scansione completa del computer dalla finestra principale, viene avviata l'esecuzione del modulo di questa attività.

OGGETTO INFETTO

Oggetto contenente codice dannoso. Il rilevamento di un oggetto contenente codice dannoso avviene quando una sezione del codice dell'oggetto corrisponde in modo preciso a una sezione del codice di una minaccia nota. Kaspersky Lab sconsiglia l'uso di oggetti di questo tipo poiché potrebbe causare un'infezione nel computer.

OGGETTO OLE

Un oggetto allegato o un oggetto incorporato in un altro file. L'applicazione Kaspersky Lab consente di esaminare gli oggetti OLE alla ricerca di virus. Se ad esempio si inserisce una tabella di Microsoft Office Excel in un documento di Microsoft Office Word, tale tabella verrà esaminata come oggetto OLE.

OGGETTO PERICOLOSO

Oggetti contenenti un virus. Si sconsiglia di accedere a questi oggetti perché ciò potrebbe determinare un'infezione del computer. Una volta rilevato un oggetto infetto, si consiglia di disinfettarlo tramite una delle applicazioni di Kaspersky Lab o di eliminarlo se l'operazione non può essere eseguita.

OGGETTO POTENZIALMENTE INFETTABILE

Un oggetto che, a causa della sua struttura o formato, può essere utilizzato dagli intrusi come "contenitore" per memorizzare e distribuire un oggetto dannoso. Di regola, si tratta di file eseguibili, ad esempio file con estensione **com**, **exe**, **dll** e così via. Il rischio di attivare codice dannoso in tali file è estremamente alto.

OGGETTO POTENZIALMENTE INFETTO

Un oggetto contenente codice modificato di un virus noto, oppure codice che ricorda quello di un virus, ma non ancora noto a Kaspersky Lab. I file potenzialmente infetti vengono rilevati tramite l'analizzatore euristico.

OGGETTO SOSPETTO

Un oggetto contenente codice modificato di un virus noto, oppure codice che ricorda quello di un virus, ma non ancora noto a Kaspersky Lab. Gli oggetti sospetti vengono rilevati mediante l'analisi euristica.

OGGETTI DI AVVIO

Il set di programmi necessario per avviare e far funzionare correttamente il sistema operativo e il software installato nel computer. Questi oggetti vengono eseguiti a ogni avvio del sistema operativo. Esistono virus in grado di infettare questi tipi di oggetti in particolare e bloccare, ad esempio, l'accesso al sistema operativo.

PACCHETTO DI AGGIORNAMENTO

Pacchetto di file per l'aggiornamento del software. Viene scaricato da Internet e installato nel computer.

PERIODO DI VALIDITÀ DELLA LICENZA

Periodo di tempo durante il quale è possibile utilizzare tutte le funzionalità dell'applicazione Kaspersky Lab. Il periodo di validità della licenza in genere ha la durata di un anno a partire dalla data di installazione. Allo scadere della licenza, l'applicazione funziona con un numero ridotto di funzioni e non è più possibile aggiornare i database dell'applicazione.

PORTA DI INPUT/OUTPUT

Viene utilizzata nei processori, ad esempio Intel, per lo scambio di dati con componenti hardware. Una porta di input/output viene associata a un determinato componente hardware e consente alle applicazioni di effettuare lo scambio di dati.

PORTA DI RETE

Parametro TCP e UDP che determina la destinazione dei pacchetti di dati in formato IP trasmessi a un host tramite una rete e che rende possibile l'esecuzione di vari programmi su un host unico per ricevere i dati indipendentemente l'uno dall'altro. Ogni programma elabora i dati ricevuti attraverso una determinata porta. Talvolta viene definito il programma "in ascolto" sulla porta.

Per alcuni protocolli di rete comuni, esistono in genere numeri di porta standard (ad esempio i server Web in genere ricevono richieste HTTP sulla porta TCP 80). I programmi possono tuttavia utilizzare qualsiasi protocollo su qualsiasi porta. Valori possibili: da 1 a 65535.

PORTA HARDWARE

Socket su un componente hardware di un computer in cui è possibile collegare un cavo o una spina (porta LPT, porta seriale, porta USB).

PROCESSO ATTENDIBILE

Processo dell'applicazione le cui operazioni non sono monitorate dall'applicazione di Kaspersky Lab nella modalità di protezione in tempo reale. In altre parole, nessun oggetto eseguito, aperto o salvato dal processo considerato attendibile verrà esaminato.

PROTEZIONE IN TEMPO REALE

Modalità operativa dell'applicazione che consente di eseguire la scansione degli oggetti per verificare la presenza di codice dannoso in tempo reale.

L'applicazione intercetta tutti i tentativi di aprire qualsiasi oggetto (lettura, scrittura o esecuzione) ed esegue una scansione di quest'ultimo per verificare la presenza di minacce. Gli oggetti non infetti vengono passati all'utente, quelli contenenti minacce o nei quali si sospetta la presenza di una minaccia vengono elaborati in base alle impostazioni dell'attività e quindi disinfettati, eliminati o messi in Quarantena.

PROTOCOLLO

Set di regole chiaramente definite e standardizzate che regolano l'interazione tra un client e un server. I protocolli più conosciuti e i servizi ad essi associati includono HTTP (WWW), FTP e NNTP (news).

QUARANTENA

Una cartella nella quale vengono conservati tutti gli oggetti potenzialmente infetti rilevati durante le scansioni o la protezione in tempo reale.

RIPRISTINO

Spostamento di un oggetto originale dalla sezione Quarantena o Backup alla cartella in cui era stato inizialmente trovato prima di essere spostato nella Quarantena, disinfettato, eliminato o in una cartella diversa specificata dall'utente.

SCANSIONE DEL TRAFFICO

Scansione in tempo reale che utilizza informazioni dell'ultima versione dei database per gli oggetti trasmessi attraverso tutti i protocolli, ad esempio HTTP, FTP e così via.

SCRIPT

Piccolo programma per computer o una parte indipendente del programma (funzione) che in genere viene sviluppata per eseguire un'attività specifica di portata ridotta. Vengono spesso utilizzati con programmi incorporati in ipertesti. Gli script vengono eseguiti, ad esempio, quando si aprono determinati siti Web.

Se è abilitata la protezione in tempo reale, l'applicazione controllerà l'avvio degli script, intercettandoli ed esaminandoli alla ricerca di virus. In funzione dei risultati della scansione, è possibile bloccare o eliminare l'esecuzione degli script.

SERVER DEGLI AGGIORNAMENTI DI KASPERSKY LAB

Elenco dei server HTTP e FTP di Kaspersky Lab da cui l'applicazione scarica database e aggiornamenti dei moduli nel computer.

SERVER PROXY

Servizio di rete del computer che consente agli utenti di effettuare richieste indirette ad altri servizi di rete. Innanzitutto, un utente si connette a un server proxy e richiede una risorsa, ad esempio un file, che si trova in un altro server. Quindi il server proxy si connette al server specificato e ottiene la risorsa desiderata o restituisce la risorsa dalla relativa cache, qualora il proxy ne preveda una. In alcuni casi, la richiesta di un utente o la risposta di un server può essere modificata dal server proxy per determinati motivi.

SETTORE DI AVVIO DEL DISCO

Un settore di avvio è una determinata area sul disco rigido, su floppy o su altri dispositivi di memorizzazione dei dati. Contiene informazioni sul file system del disco e un programma di caricamento responsabile dell'avvio del sistema operativo.

Esistono diversi virus che infettano i settori di avvio e definiti di conseguenza virus di boot. L'applicazione di Kaspersky Lab consente di esaminare i settori di avvio alla ricerca di virus e di disinfettarli se viene rilevata un'infezione.

SOCKS

Protocollo del server proxy che consente di stabilire una connessione punto-punto tra computer nelle reti interne ed esterne.

SOGLIA DI ATTIVITÀ DEI VIRUS

Livello massimo consentito di un tipo specifico di evento in un periodo di tempo limitato che, se superato, verrà considerato come attività eccessiva del virus e minaccia di un attacco di virus. Questa funzionalità è molto importante durante gli attacchi di virus e consente a un amministratore di reagire con tempestività alle minacce di attacchi che si presentano.

SPOSTAMENTI DI OGGETTI NELLA QUARANTENA

Metodo di elaborazione di un oggetto potenzialmente infetto attraverso il blocco dell'accesso al file e lo spostamento dalla posizione originale alla cartella Quarantena, in cui viene salvato in forma crittografata, in modo da eliminare la minaccia di infezione.

STATO DELLA PROTEZIONE

Stato corrente della protezione che indica il livello di sicurezza del computer.

TECNOLOGIA iCHECKER

iChecker è una tecnologia che consente di accelerare la scansione anti-virus escludendo gli oggetti che sono rimasti inalterati dall'ultima scansione, sempre che i parametri di scansione, ovvero le impostazioni e il database anti-virus, non siano stati modificati. Le informazioni di ogni file vengono archiviate in un database speciale. Questa tecnologia viene utilizzata nelle modalità di protezione in tempo reale e di scansione a richiesta.

Si supponga, ad esempio, che a un archivio esaminato da Kaspersky Anti-Virus sia stato assegnato lo stato *non infetto*. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se il contenuto dell'archivio è stato modificato aggiungendo un nuovo oggetto, oppure sono state modificate le impostazioni di scansione o è stato aggiornato il database anti-virus, l'archivio verrà esaminato nuovamente.

Limitazioni della tecnologia iChecker:

- questa tecnologia non rappresenta la scelta ideale con i file di grandi dimensioni in quanto risulta più veloce esaminare un file che controllare se sia stato modificato dall'ultima scansione;
- la tecnologia supporta un numero limitato di formati (**exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar**).

VIRUS DI BOOT

Virus che infetta i settori di avvio dell'unità disco rigido di un computer. Il caricamento del virus all'interno del sistema viene forzato durante il riavvio dal virus stesso e il codice del virus assume il controllo diretto al posto del codice del programma di avvio originale.

VIRUS SCONOSCIUTO

Nuovo virus su cui non sono disponibili informazioni nei database. In genere i virus sconosciuti vengono rilevati dall'applicazione negli oggetti mediante l'analisi euristica e tali oggetti vengono classificati come potenzialmente infetti.

KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab rappresenta oggi una delle aziende leader nello sviluppo di una vasta gamma di prodotti software ad elevate prestazioni destinati alla protezione delle informazioni, tra cui sistemi anti-virus, anti-spam e anti-hacking.

Kaspersky Lab è una società internazionale. La sede centrale si trova a Mosca, in Russia, con uffici distaccati nel Regno Unito, in Francia, Germania, Italia, Spagna, Olanda, Polonia, Giappone, Cina, Corea, Romania e negli USA (California). Recentemente è stata inaugurata una nuova sede, l'European Anti-Virus Research Centre, in Francia. La rete di partner di Kaspersky Lab è costituita da oltre 500 aziende in tutto il mondo.

Degli oltre 1000 specialisti qualificati che lavorano presso Kaspersky Lab, 10 hanno conseguito un Master di specializzazione post laurea in Business Administration e 16 un dottorato di ricerca. Gli esperti anti-virus Kaspersky Lab collaborano attivamente con altre associazioni IT CARO (Computer Anti-Virus Research Organization) e ICSA (International Computer Security Association). Kaspersky Lab è anche un partner di SUSE e Red Hat.

I punti di forza dell'azienda sono la notevole competenza e la significativa esperienza maturata in anni di intensa attività di sviluppo di soluzioni anti-virus efficaci. Un'analisi approfondita delle attività dei virus informatici consente agli specialisti dell'azienda di anticipare le tendenze nello sviluppo di malware e di offrire agli utenti una protezione efficace e tempestiva contro nuovi tipi di attacchi. Questo vantaggio sta alla base dei prodotti e dei servizi offerti da Kaspersky Lab. I prodotti dell'azienda sono sempre un passo avanti rispetto a quelli della concorrenza nell'ambito della protezione anti-virus.

L'esperienza maturata in questi anni hanno rafforzato nel tempo la posizione dominante raggiunta oggi. Kaspersky Lab è stata la prima azienda a sviluppare molti degli standard per software anti-virus moderni. Il prodotto di punta, Kaspersky Anti-Virus®, protegge in modo efficace tutti i tipi di sistemi dagli attacchi dei virus, incluse le workstation, i file server, i sistemi di posta, i firewall, i gateway Internet e i computer palmari. Gli strumenti di facile gestione di cui è fornito consentono di automatizzare la protezione anti-virus di computer e reti aziendali. Un gran numero di sviluppatori di fama internazionale utilizza il kernel di Kaspersky Anti-Virus nei propri prodotti, inclusi Nokia ICG (USA), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India) e BorderWare (Canada).

I clienti di Kaspersky Lab possono usufruire di una vasta gamma di servizi aggiuntivi che garantiscono il funzionamento costante dei prodotti e una conformità completa ai propri requisiti aziendali specifici. L'azienda progetta, implementa e supporta sistemi anti-virus aziendali. Il database anti-virus di Kaspersky Lab viene aggiornato ogni ora. Il servizio di supporto tecnico offerto ai clienti è disponibile 24 ore su 24, in diverse lingue.

Per porre domande, fare commenti o ricevere consigli, è possibile contattarci tramite i rivenditori o direttamente presso Kaspersky Lab. Tutta l'assistenza necessaria in relazione alle questioni sollevate sui prodotti di Kaspersky Lab verrà fornita tramite telefono o posta elettronica. Verrà sempre garantita una risposta completa e dettagliata a qualsiasi domanda.

Sito ufficiale di Kaspersky Lab: <http://www.kaspersky.it>

Enciclopedia dei Virus: <http://www.viruslist.com>

Anti-Virus Lab: newvirus@kaspersky.com
(solo per l'invio di oggetti sospetti negli archivi)
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=it>
(per l'invio di richieste agli analisi anti-virus)

Forum Web Kaspersky Lab: <http://forum.kaspersky.com>

CONTRATTO DI LICENZA

AVVERTENZA LEGALE IMPORTANTE PER TUTTI GLI UTENTI: LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO PRIMA DI INIZIARE A USARE IL SOFTWARE.

FACENDO CLIC SUL PULSANTE ACCETTO NELLA FINESTRA DEL CONTRATTO DI LICENZA O IMMETTENDO IL/ SIMBOLO/I CORRISPONDENTE/I, LEI ACCETTA DI ESSERE VINCOLATO AL RISPETTO DEI TERMINI E DELLE CONDIZIONI DI QUESTO CONTRATTO. **TALE AZIONE EQUIVALE AD APPORRE LA SUA FIRMA E SIGNIFICA CHE ACCETTA DI ESSERE VINCOLATO E DI DIVENTARE UNA PARTE CONTRAENTE DEL PRESENTE CONTRATTO E CHE ACCETTA LA VALIDITÀ LEGALE DEL PRESENTE CONTRATTO COME QUALSIASI ACCORDO STIPULATO PER ISCRITTO E DA LEI FIRMATO.** SE NON È D'ACCORDO CON TUTTI I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO, ANNULLI L'INSTALLAZIONE DEL SOFTWARE E NON LO INSTALLI.

DOPO AVER CLICCATO IL PULSANTE "ACCETTO" NELLA FINESTRA DEL CONTRATTO DI LICENZA O DOPO AVER IMMESSO IL/ SIMBOLO/I CORRISPONDENTE/I LEI HA IL DIRITTO DI USARE IL SOFTWARE SECONDO I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO.

1. Definizioni

- 1.1. **Per Software** si intende il software, compresi gli aggiornamenti e i relativi materiali.
- 1.2. **Per Titolare** (titolare di tutti i diritti, sia esclusivi che non, relativi al Software) si intende Kaspersky Lab ZAO, una società regolarmente costituita ai sensi delle leggi della Federazione Russa.
- 1.3. **Per Computer** si intende l'hardware, ivi compresi i personal computer, i laptop, le postazioni di lavoro, i personal digital assistant, gli "smart phone", i dispositivi palmari o gli altri dispositivi elettronici per cui il Software è stato progettato su cui il Software verrà installato e/o utilizzato.
- 1.4. **Per Utente Finale (Lei/Suo)** si intende il soggetto o i soggetti che installano o utilizzano il Software per proprio conto e che sta/stanno utilizzando legalmente una copia del Software; o, se il Software è stato scaricato o installato per conto di un'organizzazione, ad esempio da un dipendente, "*Lei*" sta a intendere anche l'organizzazione per cui il Software è stato scaricato o installato e si dichiara con il presente che tale organizzazione ha autorizzato quel soggetto ad accettare questo contratto, scaricando e installando il Software per conto dell'organizzazione stessa. Ai fini del presente contratto il termine "*organizzazione*" include, a titolo esemplificativo e non limitativo, qualsiasi società di persone, società a responsabilità limitata, persona giuridica, associazione, società per azioni, trust, joint venture, organizzazione sindacale, organizzazione non registrata o autorità governativa.
- 1.5. **Per Partner** si intendono le organizzazioni o il soggetto/i soggetti che distribuiscono il Software al Titolare sulla base di un contratto e di una licenza.
- 1.6. **Per Aggiornamento/i** si intendono tutti gli aggiornamenti, le revisioni, le patch, i perfezionamenti, le correzioni, le modifiche, le copie, le aggiunte o i pacchetti di manutenzione, ecc.
- 1.7. **Per Manuale dell'Utente** si intende il manuale dell'utente, la guida per l'amministratore, il libro di riferimento e i relativi materiali di tipo illustrativo o di altro tipo.

2. Concessione della licenza

- 2.1. Con il presente il Titolare Le concede licenza di uso non esclusivo per la memorizzazione, il caricamento, l'installazione, l'esecuzione e la visualizzazione (l'"uso") del Software su di una quantità specificata di Computer al fine di fornire un supporto per la protezione del Suo Computer, sul quale è installato il Software, contro le minacce descritte nel Manuale dell'Utente, in osservanza di tutti i requisiti tecnici descritti nel Manuale dell'Utente e secondo i termini e le condizioni di questo Contratto (la "Licenza") e Lei accetta questa Licenza:

Versione di prova. Se ha ricevuto, scaricato e/o installato la versione di prova del Software e se ha aderito alla licenza di valutazione del Software, può utilizzare il Software solo a scopo dimostrativo e soltanto per il periodo dimostrativo consentito, salvo laddove diversamente indicato, a partire dalla data della prima installazione. È severamente proibito l'uso del Software per scopi diversi o per un periodo più lungo del periodo di valutazione consentito.

Software per ambiente multiplo: Software a linguaggio multiplo: Software a doppio supporto magnetico: Copie multiple: Servizi aggiuntivi. Qualora Lei utilizzi diverse versioni del Software o edizioni del Software di lingua diversa, o riceva il Software su diversi supporti magnetici, o comunque riceva copie multiple del Software, ovvero qualora in cui Lei abbia acquistato il Software insieme a software aggiuntivi, il numero massimo di Computer su cui il Software può essere installato equivale al numero di licenze ricevuto dal Titolare *sempre che* ogni licenza acquistata Le dia diritto a installare e utilizzare il Software sulla quantità numero di Computer specificata nei paragrafi 2.2 e 2.3, salvo laddove diversamente stabilito dai termini della licenza.

- 2.2. Se il Software è stato acquistato su un supporto fisico, Lei ha il diritto di utilizzare il Software per proteggere la quantità di Computer specificata nel pacchetto Software.
- 2.3. Se il Software è stato acquistato via Internet, Lei ha il diritto di utilizzare il Software per la protezione della quantità di Computer specificata all'atto dell'acquisto della Licenza del Software.
- 2.4. Lei ha diritto di copiare il Software soltanto a scopo di back-up e solo a titolo di sostituzione della copia di Sua legale proprietà, qualora essa vada persa, distrutta o diventi inutilizzabile. Questa copia di back-up non può essere utilizzata per fini diversi e deve essere distrutta quando viene meno il diritto d'uso del Software o alla scadenza della Sua licenza o qualora questa venga meno per qualsiasi altro motivo, ai sensi dalla legislazione in vigore nel principale paese di residenza o nel paese in cui Lei fa uso del Software.
- 2.5. Lei ha la facoltà di trasferire il diritto non esclusivo di licenza d'uso del Software ad altri soggetti o persone giuridiche previste dalla licenza concessaLe dal Titolare, purché il beneficiario accetti di essere vincolato da tutti i termini e dalle condizioni del presente Contratto e La sostituisca in toto nel godimento della licenza concessa dal Titolare. In caso di trasferimento di tutti i diritti d'uso del Software concessi dal Titolare, Lei è tenuto a distruggere tutte le copie del Software, ivi compresa la copia di back-up. Se Lei è il beneficiario della licenza così trasferita, deve accettare di osservare tutti i termini e le condizioni del presente Contratto. Se Lei non accetta di essere vincolato da tutti i termini e le condizioni del presente Contratto, non Le è permesso installare e/o fare uso del Software. In qualità di beneficiario della licenza trasferita, Lei riconosce inoltre di non detenere altri diritti o diritti migliori rispetto a quelli che spettavano all'Utente Finale che ha acquistato il Software dal Titolare.
- 2.6. Dal momento in cui si procede all'attivazione del Software o dopo l'installazione del file della chiave di licenza (a eccezione della versione di prova del Software), Lei ha diritto di ricevere i seguenti servizi per il periodo di tempo specificato sul pacchetto Software (se il Software è stato acquistato su supporto fisico) o specificato durante l'acquisto (se il Software è stato acquistato via Internet):
 - Aggiornamenti del Software via Internet quando e nel momento in cui il Titolare li pubblica sul suo sito o attraverso altri servizi online. Qualsiasi Aggiornamento di cui Lei possa essere destinatario costituisce parte del Software e a esso si applicano i termini e le condizioni di questo Contratto;
 - Supporto Tecnico via Internet e Hotline telefonica di Supporto Tecnico.

3. Attivazione e validità

- 3.1. Nel caso in cui Lei apportasse modifiche al Suo computer o al software di altri fornitori installato su di esso, il Titolare ha la facoltà di chiederLe di ripetere l'attivazione del Software o l'installazione del file della chiave di licenza. Il Titolare si riserva il diritto di utilizzare qualsiasi mezzo e qualsiasi procedura per verificare la validità della Licenza e/o la validità legale della copia del Software installata e/o utilizzata sul Suo Computer.
- 3.2. Se il Software è stato acquistato su supporto fisico, esso può essere utilizzato previa accettazione del presente Contratto per il periodo specificato sulla confezione a far data dalla data di accettazione del presente Contratto.
- 3.3. Se il Software è stato acquistato via Internet, il Software può essere utilizzato previa accettazione del presente Contratto per il periodo specificato durante l'acquisto.
- 3.4. Lei ha diritto di usare la versione di prova del Software secondo quanto disposto dal Paragrafo 2.1 senza alcun addebito unicamente per il periodo di valutazione (30 giorni) concesso dal momento della sua attivazione ai sensi del presente Contratto, *purché* la versione di prova non dia diritto ad Aggiornamenti e a Supporto Tecnico via Internet e tramite Hotline telefonica.
- 3.5. La Sua Licenza d'Uso del Software è limitata al periodo di tempo specificato nei Paragrafi 3.2 o 3.3 (secondo quanto applicabile) e nel periodo restante può essere visionata utilizzando i supporti descritti nel Manuale dell'Utente.

- 3.6. Nel caso in cui Lei abbia acquistato il Software per un utilizzo su più di un Computer, la Sua Licenza d'Uso del Software è limitata al periodo di tempo che ha inizio alla data di attivazione del Software o l'installazione del file della chiave di licenza sul primo Computer.
- 3.7. Fatto salvo qualsiasi altro rimedio previsto dalla legge o basato sui principi di opportunità, giustizia e onesta composizione ("equity") a cui il Titolare possa legittimamente fare ricorso, nel caso di una Sua violazione dei termini e delle condizioni del presente Contratto, il Titolare avrà diritto in ogni momento e senza obbligo di preavviso di rescindere questa Licenza d'uso del Software senza rimborsare il prezzo d'acquisto né parte di esso.
- 3.8. Lei accetta di fare uso del Software e utilizzare qualsiasi rapporto o informazione derivante dall'utilizzo di questo Software in modo conforme a tutte le leggi applicabili internazionali, nazionali, statali, regionali e locali e a qualsiasi normativa, ivi compresa, a titolo esemplificativo e non limitativo, le leggi sulla privacy, sui diritti d'autore, sul controllo delle esportazioni e sulle oscenità.
- 3.9. Fatte salve eventuali disposizioni contrarie specificamente previste in questa sede, Lei non ha la facoltà di trasferire né di assegnare alcuno dei diritti che le sono stati concessi ai sensi del presente Contratto né alcuno degli obblighi che da esso Le derivano.

4. Supporto Tecnico

Il Supporto Tecnico descritto al Paragrafo 2.6 del presente Contratto Le viene fornito quando è stato installato l'Aggiornamento più recente del Software (a eccezione della versione di prova del Software). Servizio di assistenza tecnica: <http://support.kaspersky.com>

5. Raccolta di informazioni

- 5.1. Avendo accettato i termini e le condizioni del presente Contratto, Lei accetta di fornire informazioni al Titolare sui file eseguibili e sulle relative *checksum* allo scopo di migliorare il livello degli accorgimenti di sicurezza a Sua disposizione.
- 5.2. Allo scopo di migliorare la consapevolezza in materia di sicurezza circa le nuove minacce e le loro origini e allo scopo di migliorare il livello degli accorgimenti di sicurezza a Sua disposizione, con il Suo consenso, che è stato esplicitamente confermato nella Dichiarazione della Raccolta dei Dati del Kaspersky Security Network, Lei ha espressamente il diritto di ottenere tali informazioni. Lei può disattivare il servizio Kaspersky Security Network durante l'installazione. Inoltre, Lei può attivare e disattivare il servizio Kaspersky Security Network in qualsiasi momento nella pagina delle opzioni del Software.

Inoltre, Lei dichiara e accetta che qualsiasi informazione raccolta dal Titolare possa essere usata per monitorare e pubblicare relazioni sui trend relativi ai rischi per la sicurezza, a sola e unica discrezione del Titolare.

- 5.3. Il Software non elabora alcun dato che possa essere personalmente identificabile e non abbina i dati in elaborazione ad alcuna informazione personale.
- 5.4. Se non desidera che le informazioni raccolte dal Software vengano inviate al Titolare, non deve attivare e/o disattivare il servizio Kaspersky Security Network.

6. Restrizioni

- 6.1. Le è fatto divieto di emulare, clonare, locare, dare in prestito, noleggiare, vendere, modificare, decompilare o reingegnerizzare il Software, disassemblarlo o creare opere accessorie basate sul Software o su una porzione di esso con la sola eccezione di diritti non rinunciabili previsti dalla legislazione applicabile, e Le è fatto comunque divieto di ridurre parte del Software in forma decifrabile o trasferire il Software tutelato da licenza o qualsivoglia sottoinsieme dello stesso, o permettere a terzi di fare quanto sopra, salvo nella misura in cui le limitazioni sopra illustrate siano espressamente proibite dal diritto applicabile. È fatto divieto di utilizzare o reingegnerizzare qualsivoglia codice binario o origine del Software allo scopo di ricreare l'algoritmo del programma, che è proprietario. Tutti i diritti non espressamente concessi attraverso il presente Contratto sono riservati al Titolare e/o ai suoi fornitori, secondo quanto applicabile. L'uso non autorizzato del Software produrrà la rescissione immediata e automatica del presente Contratto e della Licenza concessa in virtù dello stesso e può determinare l'apertura di un procedimento legale nei Suoi confronti.
- 6.2. Fatto salvo quanto disposto al Paragrafo 2.5 del presente Contratto, Lei non ha diritto di trasferire i diritti d'uso del Software a terzi.

- 6.3. Le è fatto divieto di mettere a conoscenza di terzi il codice di attivazione e/o il file chiave della licenza o di consentire l'accesso al codice di attivazione e/o di licenza, i quali rappresentano dati riservati del Titolare; Lei sarà inoltre tenuto a usare ogni ragionevole cautela per la protezione del codice di attivazione e/o di licenza riservati, qualora Lei abbia la facoltà di trasferire il codice di attivazione e/o di licenza a terzi secondo quanto illustrato al Paragrafo 2.5 del presente Contratto.
- 6.4. Non è consentito concedere a noleggio, in locazione o in prestito a terzi il Software.
- 6.5. Non è consentito utilizzare il Software per la creazione di dati o di software che servono a individuare, bloccare o gestire le minacce descritte nel Manuale dell'Utente.
- 6.6. In caso di violazione dei termini e delle condizioni del presente Contratto, il Titolare ha il diritto di bloccare il file di codice o di annullare la Sua licenza d'uso del Software senza obbligo di rimborso.
- 6.7. Se si usa la versione di prova del Software non si ha il diritto di ricevere il Supporto Tecnico specificato al Paragrafo 4 del presente Contratto, né il diritto di trasferire la licenza o i diritti d'uso del software a terzi

7. Garanzia limitata e clausola di esclusione della responsabilità

- 7.1. Il Titolare garantisce che il Software eseguirà sostanzialmente le prestazioni illustrate nelle specifiche e descritte nel Manuale dell'Utente *fermo restando, tuttavia, che* tale garanzia limitata non si applica a quanto segue: (w) lacune del Suo Computer e relative violazioni per le quali il Titolare declina espressamente qualsiasi responsabilità di garanzia; (x) malfunzionamenti, difetti o guasti conseguenti a cattivo uso, abuso, incidente, negligenza, difetti di installazione, funzionamento o manutenzione, furto, atto vandalico, evento di forza maggiore, atti di terrorismo, interruzione di tensione o momentanea sovratensione, infortunio, alterazione, modifica non consentita o riparazioni eseguite da soggetti diversi dal Titolare o qualsiasi azione o causa, a opera Sua o di qualsiasi altro soggetto terzo, ragionevolmente fuori del controllo del Titolare; (y) qualsiasi difetto da Lei tenuto nascosto al Titolare anche dopo la comparsa della prima anomalia; e (z) incompatibilità provocata da componenti hardware e/o software installati sul Suo computer.
- 7.2. Lei riconosce, accetta e concorda che nessun software è esente da errori e che Lei è stato informato che è necessario fare il back-up del Computer, con la frequenza e secondo le modalità per Lei più indicate.
- 7.3. In caso di violazione dei termini descritti nel Manuale dell'Utente o nel presente Contratto, il Titolare non garantisce il corretto funzionamento del Software.
- 7.4. Il Titolare non garantisce che il Software funzionerà correttamente se Lei non scarica regolarmente gli Aggiornamenti specificati nel Paragrafo 2.6 del presente Contratto.
- 7.5. Il Titolare non garantisce la protezione dalle minacce descritte nel Manuale dell'Utente una volta scaduto il periodo specificato nei Paragrafi 3.2 or 3.3 del presente Contratto o una volta scaduta, per qualsiasi motivo, la Licenza d'uso del Software.
- 7.6. IL SOFTWARE VIENE FORNITO "COSÌ COM'È" E IL TITOLARE NON FA ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA IN QUANTO A USO O PRESTAZIONI. FATTE SALVE LE GARANZIE, LE CONDIZIONI, LE DICHIARAZIONI O I TERMINI CHE NON POSSONO ESSERE ESCLUSI O LIMITATI DAL DIRITTO APPLICABILE, IL TITOLARE E I SUOI PARTNER, NON FORNISCONO ALCUNA GARANZIA, CONDIZIONE, DICHIARAZIONE O TERMINE (NÉ ESPLICITO NÉ IMPLICITI NÉ PREVISTO DALLA LEGGE, DALLA *COMMON LAW*, DALLE CONSUETUDINI O DAGLI USI O ALTRO) IN MERITO A QUALSIVOGLIA QUESTIONE, IVI COMPRESA, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, LA NON VIOLAZIONE DEI DIRITTI DI TERZI, LA COMMERCIALIZZABILITÀ, LA QUALITÀ SODDISFACENTE, L'INTEGRAZIONE O L'APPLICABILITÀ PER UN FINE SPECIFICO. LEI SI ASSUME LA RESPONSABILITÀ DI TUTTI GLI ERRORI E TUTTI I RISCHI RELATIVI ALLE PRESTAZIONI NONCHÉ LA RESPONSABILITÀ DI AVER SCELTO IL SOFTWARE ALLO SCOPO DI RAGGIUNGERE I RISULTATI DESIDERATI NONCHÉ DELL'INSTALLAZIONE DEL SOFTWARE, DEL RELATIVO USO E DEI RISULTATI OTTENUTI DALLO STESSO. SENZA LIMITARE LE DISPOSIZIONI DI CUI SOPRA, IL TITOLARE NON FORNISCE ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA CHE IL SOFTWARE SARÀ ESENTE DA ERRORI O ESENTE DA INTERRUZIONI O ALTRI DIFETTI DI FUNZIONAMENTO NÉ CHE IL SOFTWARE SARÀ IN GRADO DI SODDISFARE IN TOTO O IN PARTE LE SUE ESIGENZE, SIANO ESSE STATE COMUNICATE AL TITOLARE O MENO.

8. Esclusione e limite della responsabilità

NELLA MASSIMA MISURA CONSENTITA DAL DIRITTO APPLICABILE, IN NESSUN CASO IL TITOLARE O I SUOI PARTNER SARANNO RESPONSABILI DI DANNI SPECIALI, MARGINALI, PUNITIVI, INDIRETTI O DI DANNI INDIRETTI DI QUALSIASI TIPO (IVI COMPRESI, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, I DANNI PER PERDITA DI UTILI O PER PERDITA DI INFORMAZIONI RISERVATE O DI ALTRE INFORMAZIONI, PER INTERRUZIONE DELL'ATTIVITÀ LAVORATIVA, PER PERDITA DI PRIVACY, PER CORRUZIONE, DANNO E PERDITA DI DATI O DI PROGRAMMI, PER MANCATA OSSERVANZA DI UN OBBLIGO IVI COMPRESO QUALSIASI ONERE IMPOSTO PER LEGGE, DOVERE DI BUONA FEDE O DOVERE DI RAGIONEVOLE DILIGENZA, PER NEGLIGENZA, PER PERDITA ECONOMICA E PER QUALSIASI ALTRA PERDITA PECUNIARIA O ALTRA PERDITA DI SORTA) DERIVANTE DA O IN QUALSIASI MODO COLLEGATO ALL'USO O ALL'IMPOSSIBILITÀ DI USARE IL SOFTWARE, ALLA FORNITURA O MANCATA FORNITURA DEL SERVIZIO DI SUPPORTO O DI ALTRI SERVIZI, INFORMAZIONI, SOFTWARE E RELATIVI CONTENUTI ATTRAVERSO IL SOFTWARE O COMUNQUE DERIVANTI DALL'USO DEL SOFTWARE O COMUNQUE AI SENSI O IN RELAZIONE A QUALSIASI DISPOSIZIONE DEL PRESENTE CONTRATTO, O DERIVANTI DA UNA VIOLAZIONE DEL PRESENTE CONTRATTO O DA QUALSIVOGLIA ILLECITO (IVI COMPRESA LA NEGLIGENZA, LA FALSA TESTIMONIANZA, QUALSIASI OBBLIGO O DOVERE RELATIVI ALLA RESPONSABILITÀ) O DA UNA VIOLAZIONE DI UN OBBLIGO DI LEGGE O DA UNA VIOLAZIONE DELLA GARANZIA DA PARTE DEL TITOLARE O DI UNO DEI SUOI PARTNER, ANCHE QUALORA IL TITOLARE O UNO DEI SUOI PARTNER SIA STATO INFORMATO DELLA POSSIBILITÀ DI TALI DANNI.

LEI ACCETTA CHE NEL CASO IN CUI IL TITOLARE E/O SUOI PARTNER VENISSE TROVATI RESPONSABILI, LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER SI LIMITERÀ AL COSTO DEL SOFTWARE. IN NESSUN CASO LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER POTRÀ SUPERARE LE SOMME VERSATE PER IL SOFTWARE AL TITOLARE O AL PARTNER (SECONDO QUANTO APPLICABILE).

NULLA IN QUESTO CONTRATTO ESCLUDE O LIMITA LA QUALSIVOGLIA RICHIESTA DI DANNI IN CASO DI MORTE E LESIONI PERSONALI. INOLTRE IN CASO IN CUI UNA MANLEVA, ESCLUSIONE O LIMITAZIONE CONTEMPLATA DAL PRESENTE CONTRATTO NON POSSA ESSERE ESCLUSA O LIMITATA AI SENSI DEL DIRITTO APPLICABILE, QUELLA MANLEVA, ESCLUSIONE O LIMITAZIONE NON SARÀ VALIDA NEI SUOI CONFRONTI E LEI DOVRÀ CONTINUARE A OSSERVARE TUTTE LE RESTANTI MANLEVE, ESCLUSIONI E LIMITAZIONI.

9. GNU e altre licenze di Terzi

Il Software può comprendere alcuni programmi software sottoposti a licenza (o a sublicenza) dell'utente ai sensi della GNU Licenza Pubblica Generica (General Public License, GPL) o ad altra licenza software di analoga natura che, tra gli altri, concede all'utente il diritto di copiare, modificare e ridistribuire certi programmi o porzioni di essi e di avere accesso al codice source ("Software Open Source"). Se tali licenze prevedono che per un software distribuito in formato binario eseguibile anche il codice source venga reso disponibile ai suoi utenti, il codice source deve essere reso accessibile inviando la richiesta all'indirizzo source@kaspersky.com, altrimenti il codice source verrà fornito insieme al Software. Se le licenze dei Software Open Source prevedono che il Titolare fornisca diritti d'uso, di copia e modifica del programma Software Open Source più ampi dei diritti concessi in virtù del presente Contratto, tali diritti avranno la priorità sui diritti e sulle restrizioni contemplati da questo documento.

10. Proprietà Intellettuale

- 10.1 Lei accetta che il Software e il fatto di esserne autori, i sistemi, le idee e i metodi operativi, la documentazione e altre informazioni contenute nel Software, sono proprietà intellettuale esclusiva e/o preziosi segreti commerciali del Titolare o dei suoi partner e che il Titolare e i suoi partner, secondo quanto applicabile, sono protetti dal diritto civile e penale e dalla legge sul copyright, sul segreto commerciale, sul marchio di fabbrica e sui brevetti della Federazione Russa, dell'Unione Europea e degli Stati Uniti e da altri trattati internazionali o di altri paesi. Il presente Contratto non Le concede alcun diritto di proprietà intellettuale né alcun diritto sui marchi o sui marchi di servizio del Titolare e/o dei suoi partner ("Marchi di fabbrica"). Lei ha la facoltà di usare i marchi di fabbrica solo nella misura in cui essi permettono di identificare le stampe prodotte dal Software in conformità con la pratica sui marchi generalmente accettata, ivi compresa l'identificazione del nome del proprietario del Marchio di fabbrica. Tale uso di un Marchio di fabbrica non Le conferisce alcun diritto di proprietà sul Marchio stesso. Il Titolare e/o i relativi partner possiedono e conservano ogni diritto, titolo e interesse relativo e collegato al Software, ivi comprese, senza alcuna limitazione, le correzioni d'errore, i perfezionamenti, gli Aggiornamenti o altre modifiche del Software, sia apportate dal Titolare che da Terzi nonché tutti i diritti d'autore, i brevetti, i diritti su segreti commerciali, i marchi di fabbrica e qualsiasi altro diritto di proprietà intellettuale ivi contemplato. Il possesso, l'installazione o l'uso del Software da parte Sua non Le trasferisce alcun titolo nella proprietà intellettuale del Software e Lei non acquisirà alcun diritto sul Software, salvo nella misura espressamente indicata nel presente Contratto. Tutte le copie del Software eseguite ai sensi del presente documento devono contenere le stesse avvertenze proprietarie che compaiono sul e nel Software. Fatto salvo quanto disposto in questo documento, il presente Contratto non Le conferisce alcun diritto di proprietà intellettuale sul Software e Lei riconosce che la Licenza, secondo la definizione data in seguito, concessa ai sensi del presente Contratto Le conferisce soltanto il diritto di uso limitato ai termini e alle condizioni del presente Contratto. Il Titolare si riserva tutti i diritti che non Le sono espressamente concessi ai sensi del presente Contratto.

- 10.2 Lei riconosce che il codice source, il codice di attivazione e/o il file di codice di licenza per il Software sono proprietari del Titolare e che essi costituiscono segreto commerciale del Titolare. Lei accetta di non modificare, adattare, reingegnerizzare, decompilare, disassemblare, né comunque tentare di scoprire il codice source del Software.
- 10.3 Lei accetta di non modificare, né alterare in alcun modo il Software. Lei non ha la facoltà di rimuovere, né di alterare alcuna delle avvertenze in materia di diritti d'autore o altre avvertenze proprietarie sulle copie del Software.

11. Diritto applicabile; Arbitrato

Il presente Contratto sarà regolamentato dalle leggi della Federazione Russa e interpretato conformemente a esse, senza riferimento a conflitti fra stato di diritto e principi. Il presente Contratto non sarà regolamentato dalla Convenzione delle Nazioni Unite sui Contratti per la Vendita Internazionale di Merci, la cui applicazione è espressamente esclusa. Qualsiasi vertenza derivante dall'interpretazione o dall'applicazione dei termini del presente Contratto o dalla sua violazione dovrà essere regolata tramite trattativa diretta oppure dal Tribunale dell'Arbitrato Commerciale Internazionale avente sede presso la Camera di Commercio e dell'Industria della Federazione Russa di Mosca, Federazione Russa. Qualsiasi lodo arbitrale emesso dall'arbitro sarà definitivo e vincolante per le parti e qualsiasi giudizio su tale lodo può essere fatto valere in ogni foro competente. Nulla nel presente Paragrafo 11 può impedire a una delle Parti di ricercare e ottenere equo indennizzo presso un foro competente, sia prima, durante sia dopo il processo d'arbitrato.

12. Periodo di validità per la presentazione di azioni legali

A prescindere dalla forma, nessuna azione derivante dalle transazioni commerciali eseguite ai sensi del presente Contratto può essere presentata dalle due parti contrattuali a più di un (1) anno dal momento in cui è accaduto o si è scoperto che è accaduto l'evento su cui si basa l'azione, tranne in caso di azioni per violazione dei diritti di proprietà intellettuale, che possono essere presentate entro il periodo massimo applicabile secondo i termini di legge.

13. Totalità del Contratto; Clausola salvatoria; Assenza di deroga.

Il presente Contratto costituisce l'intero contratto tra Lei e il Titolare e sostituisce ogni altro accordo, proposta, comunicato o comunicato commerciale precedente, sia verbale che scritto, relativo al Software o relativo al presente Contratto. Lei riconosce di aver letto il presente Contratto, lo comprende e accetta di essere vincolato ai suoi termini e condizioni. Se un foro competente giudica una qualsiasi disposizione del presente Contratto non valida, nulla o per qualsiasi motivo non applicabile, *in toto* o in parte, tale disposizione sarà riformulata più precisamente per renderla legittima e applicabile; ciò tuttavia non inficerà il Contratto e le rimanenti disposizioni del Contratto resteranno pienamente valide e in vigore nella massima misura consentita dalla legge diritto o dall'equity, conservando quanto più possibile il loro intento originale. Non varrà alcuna deroga a disposizioni o a condizioni del presente Contratto, a meno che la deroga non sia presentata per iscritto e firmata da Lei e da rappresentante autorizzato del Titolare, purché nessuna deroga a una violazione di una disposizione del presente Contratto valga come una deroga a qualsiasi violazione precedente, concorrente o successiva. La mancata insistenza da parte del Titolare nel richiedere la stretta applicazione di qualsiasi disposizione del presente Contratto o nel far valere un diritto non potrà essere interpretata quale deroga a tale disposizione o rinuncia a tale diritto.

14. Informazioni di contatto.

Per qualsiasi domanda relativa al presente Contratto, o se si desidera consultare per qualsiasi motivo il Titolare, si prega di contattare il nostro Servizio Clienti presso:

Kaspersky Lab ZAO, 10 edificio 1 1st Volokolamsky Proezd
Mosca, 123060
Federazione Russa

Tel: +7-495-797-8700
Fax: +7-495-645-7939

E-mail: info@kaspersky.com

Sito Web: www.kaspersky.com

© 1997-2009 Kaspersky Lab ZAO. Tutti i diritti riservati. Il Software e la documentazione d'accompagnamento sono soggetti a diritto d'autore e sono protetti dalle leggi sul copyright e dai trattati internazionali sul copyright nonché da altre leggi e trattati in materia di proprietà intellettuale.

INDICE

A

Abilitazione/disabilitazione della protezione in tempo reale	96
Aggiornamento	
da una cartella locale	92
impostazioni internazionali	91
rollback dell'ultimo aggiornamento	90
sorgente degli aggiornamenti	90
utilizzo di un server proxy	91
Algoritmo di funzionamento	
Anti-Virus File	44
Anti-Virus IM	68
Anti-Virus Posta	54
Anti-Virus Web	61
Ambito di protezione	
Anti-Virus File	46
Anti-Virus IM	68
Anti-Virus Posta	56
Anti-Virus Web	63
Analisi euristica	
Anti-Virus File	47
Anti-Virus IM	69
Anti-Virus Posta	58
Anti-Virus Web	65
Anti-Virus File	
algoritmo di funzionamento	44
ambito di protezione	46
analisi euristica	47
livello di protezione	45
modalità di scansione	49
ottimizzazione della scansione	48
reazione alle minacce	45
ripristino delle impostazioni predefinite	52
scansione dei file composti	48, 49
sospensione	50, 51
tecnologia di scansione	50
Anti-Virus IM	
algoritmo di funzionamento	68
ambito di protezione	68
analisi euristica	69
database degli indirizzi Web di phishing	68
Anti-Virus Posta	
algoritmo di funzionamento	54
ambito di protezione	56
analisi euristica	58
filtraggio degli allegati	59
livello di protezione	55
reazione alle minacce	55
ripristino delle impostazioni predefinite	59
scansione dei file composti	58
Anti-Virus Web	
algoritmo di funzionamento	61
ambito di protezione	63
analisi euristica	65
Barra degli strumenti degli URL di Kaspersky	64
database degli indirizzi Web di phishing	63
livello di protezione	62

ottimizzazione della scansione	66
reazione alle minacce	62
Area attendibile	
regole di esclusione	108
Auto-difesa dell'applicazione	103

B

Barra degli URL di Kaspersky	
Anti-Virus Web	64

C

Categorie di minacce rilevabili	107
Componenti dell'applicazione	15
Configurazione del browser	125
Copia di backup	185

D

Database degli indirizzi Web di phishing	
Anti-Virus IM	68
Anti-Virus Web	63
Difesa Proattiva	
controllo degli account di sistema	72
elenco di attività pericolose	70
regole per il monitoraggio delle attività pericolose	71
Disco di ripristino	123

F

Finestra principale dell'applicazione	40
---	----

I

Icona nell'area di notifica della barra delle applicazioni	38
INTERFACCIA DELL'APPLICAZIONE	38

K

Kaspersky Anti-Virus	
avvio all'avvio del sistema operativo	96

L

Licenza	186
attiva	187
come ottenere un file di chiave della licenza	186
Limitazione dell'accesso all'applicazione	97
Livello di protezione	
Anti-Virus File	45
Anti-Virus Posta	55
Anti-Virus Web	62

M

Memoria di backup	118
Menu di scelta rapida	39

O

Oggetto infetto	188
-----------------------	-----

P

Pianificazione	
----------------	--

aggiornamento	93
scansione anti-virus	82
Prestazioni del computer	104

Q

Quarantena	117
Quarantena e backup	117

R

Rapporti	
filtraggio	133
ricerca eventi	134
salvataggio in un file	132
selezione di un componente o di un'attività	129
tipi di evento	130
RAPPORTI	128
Reazione a una minaccia	
scansione anti-virus	77
Reazione alle minacce	
Anti-Virus File	45
Anti-Virus Posta	55
Anti-Virus Web	62
Rete	
connessioni crittografate	111
Ricerca delle vulnerabilità	
elenco degli oggetti da esaminare	85
Ripristino	189
Ripristino delle impostazioni predefinite	
Anti-Virus File	52
Anti-Virus Posta	59

S

Scansione	
account	83
avvio automatico di un'attività ignorata	82
avvio di un'attività	75
azione su un oggetto rilevato	77
livello di protezione	77
ottimizzazione della scansione	79
pianificazione	82
scansione delle vulnerabilità	84
scansione di file compositi	80
tecnologie di scansione	81
tipo di oggetti da esaminare	78
Scansione Vulnerabilità	
account	87
pianificazione	86

T

Tastiera Virtuale	122
-------------------------	-----

Z

Zona attendibile	
applicazioni attendibili	107